Cyberspace Law/Law 57931
Professor Eric Goldman (formerly Eric Schlachter)
Santa Clara University School of Law
Spring 1999

1. **MEETINGS.** The class meets on Tuesday nights from 7:30 to 9:20. The first class is January 12 and the last class is April 27. Pursuant to University regulations, class will not meet on February 16 or March 2. The final exam is scheduled for May 8 at 1:15.

2. **PREREQUISITES.** This class is a general survey class in nature and thus there are no prerequisites other than completion of the first year courses. Some students have found copyright law and first amendment law classes were helpful. If you do not have experience using the Internet, you will need to gain this experience during the class.

3. **FINAL EXAM.** The class will be graded solely on the final exam. The final exam will probably be 2 hours long with either 2 or 3 questions. The exam will emphasize real life situations and problems and test your ability to come up with practical solutions.

The 1998 exam is available at http://members.theglobe.com/ericgoldman/1998final.html. The associated sample answer is at http://members.theglobe.com/ericgoldman/1998answer.html.

The 1997 exam is available at http://members.theglobe.com/ericgoldman/1997final.html. The associated sample answer is at http://members.theglobe.com/ericgoldman/finalans.html.

4. **GRADING.** Historically, I have given roughly 33% As and 10% Cs. Grading will be dependent on whether or not the class is subject to the law school's mandatory curve or if I must adjust my curve anyway.

5. **PAPERS.** No paper is required as part of the class, but many of you may be interested in writing papers or already working on papers. I would be happy to help if possible. If you are looking for a topic, consider my list of "difficult" issues at http://members.theglobe.com/ericgoldman/issues.html. You should also check out my list of cyberspace law source material. See http://members.theglobe.com/ericgoldman/tablecase.html.

6. **EMAIL LIST.** You are required to have an email account as part of the class. At the first class, I will ask you for an email address, which I will use to prepare an email list. I will use this email list for occasional class announcements, other timely messages and occasional random postings.

7. **CERTIFICATE PROGRAM.** This class is tentatively approved for credit towards the High Technology Law Certificate.

8. **OFFICE HOURS.** I do not have regular office hours on campus, but most students have found that I am very accessible by phone or email. Generally the best times to reach me are between 7 and 8:30 on Monday or Thursday evening or between 2 and 6 on Sunday afternoon. Email is usually the best way to reach me.

9. **ACADEMIC FREEDOM.** Because cyberspace permits people to be people, it is inevitable that we will discuss the seedier side of the human condition in the class. If you have any concerns about this, please let me know immediately.

10. **JOBS.** I'd like to help with your job searching efforts. We have 3 confirmed placements out of the past 2 years' classes, and already I have been asked to help fill at least one internship for Spring 1999. If you want my help, please email me your resume (in the text of an email, not as an attachment) and schedule a time to talk.

11. **PROFESSOR CONTACT INFORMATION.**

Eric Goldman (formerly Eric Schlachter)
Cooley Godward LLP
Mailing Address: 5 Palo Alto Square, 3000 El Camino Real, Palo Alto, CA 94306
Physical Address: 975 Page Mill Road, Palo Alto (subject to change in February or March)
Phone: (650) 843-5154
Fax: (650) 849-7400 (subject to change in February or March)
Work Email: egoldman@cooley.com
Personal Email: ericgoldman@theglobe.com
Web Page: http://members.theglobe.com/ericgoldman. An electronic copy of this syllabus is available at the foregoing address.

CLASS SCHEDULE AND READING MATERIALS

This class reader is the only required reading. There are a number of general mass-market summaries of cyberspace law available. Because cyberspace law is developing so rapidly, all of these books are out-of-date to some degree, and former students have not indicated a need for a supplemental reader. So, before you fork over your hard-earned cash, let me know and we can discuss the best supplemental resources for you.

1. **INTRODUCTION TO CYBERSPACE** (January 12 and 19).

2. **JURISDICTION AND VENUE** (January 26).

3. **COMMERCE CLAUSE** (January 26).

4. **ONLINE CONTRACTS** (February 2).

5. **SPAM AND TRESPASS** (February 2 and 9).

6. **ANONYMITY AND PRIVACY** (February 23).

7. **INFORMATION TORTS** (defamation, right of publicity/privacy, inaccurate information, harassment, gambling) (March 9).

8. **OBSCENITY, PORNOGRAPHY AND CHILD PORNOGRAPHY** (March 16).

9. **TRADEMARKS AND REGISTRAR LIABILITY** (March 23).

10. **COPYRIGHT, TRADE SECRET, PATENTS AND HOT NEWS** (March 30 and April 6).

11. **LIABILITY FOR THIRD PARTY CONTENT** (April 13 and 20).

12. **ECPA AND COMPUTER CRIMES** (April 27).

NOTE: Most of the readings listed above can be found electronically through http://members.theglobe.com/ericgoldman/tablecase.html, except for articles, which can be found through http://members.theglobe.com/ericgoldman/publicat.html.

In The Courts American Civil Liberties Union Freedom Network

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA
AMERICAN CIVIL LIBERTIES UNION, et al.,

v.

JANET RENO, Attorney General of
the United States

CIVIL ACTION No. 96-963

AMERICAN LIBRARY ASSOCIATION,
INC., et al.,

v.

UNITED STATES DEP'T OF JUSTICE,
et al.

CIVIL ACTION No. 96-1458

Before: Sloviter, Chief Judge, United States Court of Appeals for the Third Circuit; Buckwalter and Dalzell, Judges, United States District Court for the Eastern District of Pennsylvania

June 11, 1996

ADJUDICATION ON MOTIONS FOR PRELIMINARY INJUNCTION

I.

INTRODUCTION

Procedural Background

Before us are motions for a preliminary injunction filed by plaintiffs who challenge on constitutional grounds provisions of the Communications Decency Act of 1996 (CDA or "the Act"), which constitutes Title V of the Telecommunications Act of 1996, signed into law by the President on February 8, 1996.(1) Telecommunications Act of 1996, Pub. L. No. 104-104, § 502, 110 Stat. 56, 133-35. Plaintiffs include various organizations and individuals who, inter alia, are associated with the computer and/or communications industries, or who publish or post materials on the Internet, or belong to various citizen groups. See ACLU Complaint (¶¶ 7-26), ALA First Amended Complaint (¶¶ 3, 12-33).

The defendants in these actions are Janet Reno, the Attorney General of the United States, and the United States Department of Justice. For convenience, we will refer to these defendants as the Government. Plaintiffs contend that the two challenged provisions of the CDA that are directed to communications over the Internet which might be deemed

(3) The defenses provided in paragraph (1) of this subsection shall not be applicable to a person who provides access or connection to a facility, system, or network engaged in the violation of this section that is owned or controlled by such person.

(4) No employer shall be held liable under this section for the actions of an employee or agent unless the employee's or agent's conduct is within the scope of his or her employment or agency and the employer (A) having knowledge of such conduct, authorizes or ratifies such conduct, or (B) recklessly disregards such conduct.

(5) It is a defense to a prosecution under subsection (a)(1)(B) or (d) of this section, or under subsection (a)(2) of this section with respect to the use of a facility for an activity under subsection (a)(1)(B) that a person --

(A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or

(B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

(6) The [Federal Communications] Commission may describe measures which are reasonable, effective, and appropriate to restrict access to prohibited communications under subsection (d) of this section. Nothing in this section authorizes the Commission to enforce, or is intended to provide the Commission with the authority to approve, sanction, or permit, the use of such measures. The Commission shall have no enforcement authority over the failure to utilize such measures. . . .

II.

FINDINGS OF FACT

All parties agree that in order to apprehend the legal questions at issue in these cases, it is necessary to have a clear understanding of the exponentially growing, worldwide medium that is the Internet, which presents unique issues relating to the application of First Amendment jurisprudence and due process requirements to this new and evolving method of communication. For this reason all parties insisted on having extensive evidentiary hearings before the three-judge court. The court's Findings of fact are made pursuant to Fed. R. Civ. P. 52(a). The history and basic technology of this medium are not in dispute, and the first forty-eight paragraphs of the following Findings of fact are derived from the like-numbered paragraphs of a stipulation(8) the parties filed with the court.(9)

The Nature of Cyberspace

The Creation of the Internet and the Development of Cyberspace

1. The Internet is not a physical or tangible entity, but rather a giant network which

interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks. This is best understood if one considers what a linked group of computers -- referred to here as a "network" -- is, and what it does. Small networks are now ubiquitous (and are often called "local area networks"). For example, in many United States Courthouses, computers are linked to each other for the purpose of exchanging files and messages (and to share equipment such as printers). These are networks.

2. Some networks are "closed" networks, not linked to other computers or networks. Many networks, however, are connected to other networks, which are in turn connected to other networks in a manner which permits each computer in any network to communicate with computers on any other network in the system. This global Web of linked networks and computers is referred to as the Internet.
3. The nature of the Internet is such that it is very difficult, if not impossible, to determine its size at a given moment. It is indisputable, however, that the Internet has experienced extraordinary growth in recent years. In 1981, fewer than 300 computers were linked to the Internet, and by 1989, the number stood at fewer than 90,000 computers. By 1993, over 1,000,000 computers were linked. Today, over 9,400,000 host computers worldwide, of which approximately 60 percent located within the United States, are estimated to be linked to the Internet. This count does not include the personal computers people use to access the Internet using modems. In all, reasonable estimates are that as many as 40 million people around the world can and do access the enormously flexible communication Internet medium. That figure is expected to grow to 200 million Internet users by the year 1999.
4. Some of the computers and computer networks that make up the Internet are owned by governmental and public institutions, some are owned by non-profit organizations, and some are privately owned. The resulting whole is a decentralized, global medium of communications -- or "cyberspace" -- that links people, institutions, corporations, and governments around the world. The Internet is an international system. This communications medium allows any of the literally tens of millions of people with access to the Internet to exchange information. These communications can occur almost instantaneously, and can be directed either to specific individuals, to a broader group of people interested in a particular subject, or to the world as a whole.
5. The Internet had its origins in 1969 as an experimental project of the Advanced Research Project Agency ("ARPA"), and was called ARPANET. This network linked computers and computer networks owned by the military, defense contractors, and university laboratories conducting defense-related research. The network later allowed researchers across the country to access directly and to use extremely powerful supercomputers located at a few key universities and laboratories. As it evolved far beyond its research origins in the United States to encompass universities, corporations, and people around the world, the ARPANET came to be called the "DARPA Internet," and finally just the "Internet."
6. From its inception, the network was designed to be a decentralized, self-maintaining series of redundant links between computers and computer networks, capable of rapidly transmitting communications without direct human involvement or control, and with the automatic ability to re-route communications if one or more individual links were damaged or otherwise unavailable. Among other goals, this redundant system of linked computers was designed to allow vital research and communications to continue even if portions of the network were damaged, say, in a war.
7. To achieve this resilient nationwide (and ultimately global) communications medium, the ARPANET encouraged the creation of multiple links to and from each computer (or computer network) on the network. Thus, a computer located in Washington, D.C., might be linked (usually using dedicated telephone lines) to other computers in neighboring states or on the Eastern seaboard. Each of those computers could in turn be linked to other computers, which themselves would be linked to other computers.
8. A communication sent over this redundant series of linked computers could travel any of a number of routes to its destination. Thus, a message sent from a computer in Washington, D.C., to a computer in Palo Alto, California, might first be sent to a

computer in Philadelphia, and then be forwarded to a computer in Pittsburgh, and then to Chicago, Denver, and Salt Lake City, before finally reaching Palo Alto. If the message could not travel along that path (because of military attack, simple technical malfunction, or other reason), the message would automatically (without human intervention or even knowledge) be re-routed, perhaps, from Washington, D.C. to Richmond, and then to Atlanta, New Orleans, Dallas, Albuquerque, Los Angeles, and finally to Palo Alto. This type of transmission, and re-routing, would likely occur in a matter of seconds.

9. Messages between computers on the Internet do not necessarily travel entirely along the same path. The Internet uses "packet switching" communication protocols that allow individual messages to be subdivided into smaller "packets" that are then sent independently to the destination, and are then automatically reassembled by the receiving computer. While all packets of a given message often travel along the same path to the destination, if computers along the route become overloaded, then packets can be re-routed to less loaded computers.
10. At the same time that ARPANET was maturing (it subsequently ceased to exist), similar networks developed to link universities, research facilities, businesses, and individuals around the world. These other formal or loose networks included BITNET, CSNET, FIDONET, and USENET. Eventually, each of these networks (many of which overlapped) were themselves linked together, allowing users of any computers linked to any one of the networks to transmit communications to users of computers on other networks. It is this series of linked networks (themselves linking computers and computer networks) that is today commonly known as the Internet.
11. No single entity -- academic, corporate, governmental, or non-profit -- administers the Internet. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers). There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet.

How Individuals Access the Internet

12. Individuals have a wide variety of avenues to access cyberspace in general, and the Internet in particular. In terms of physical access, there are two common methods to establish an actual link to the Internet. First, one can use a computer or computer terminal that is directly (and usually permanently) connected to a computer network that is itself directly or indirectly connected to the Internet. Second, one can use a "personal computer" with a "modem" to connect over a telephone line to a larger computer or computer network that is itself directly or indirectly connected to the Internet. As detailed below, both direct and modem connections are made available to people by a wide variety of academic, governmental, or commercial entities.

13. Students, faculty, researchers, and others affiliated with the vast majority of colleges and universities in the United States can access the Internet through their educational institutions. Such access is often via direct connection using computers located in campus libraries, offices, or computer centers, or may be through telephone access using a modem from a student's or professor's campus or off-campus location. Some colleges and universities install "ports" or outlets for direct network connections in each dormitory room or provide access via computers located in common areas in dormitories. Such access enables students and professors to use information and content provided by the college or university itself, and to use the vast amount of research resources and other information available on the Internet worldwide.

14. Similarly, Internet resources and access are sufficiently important to many corporations and other employers that those employers link their office computer networks to the Internet

and other employers that those employers link their office computer networks to the Internet and provide employees with direct or modem access to the office network (and thus to the Internet). Such access might be used by, for example, a corporation involved in scientific or medical research or manufacturing to enable corporate employees to exchange information and ideas with academic researchers in their fields.

15. Those who lack access to the Internet through their schools or employers still have a variety of ways they can access the Internet. Many communities across the country have established "free-nets" or community networks to provide their citizens with a local link to the Internet (and to provide local-oriented content and discussion groups). The first such community network, the Cleveland Free-Net Community Computer System, was established in 1986, and free-nets now exist in scores of communities as diverse as Richmond, Virginia, Tallahassee, Florida, Seattle, Washington, and San Diego, California. Individuals typically can access free-nets at little or no cost via modem connection or by using computers available in community buildings. Free-nets are often operated by a local library, educational institution, or non-profit community group.

16. Individuals can also access the Internet through many local libraries. Libraries often offer patrons use of computers that are linked to the Internet. In addition, some libraries offer telephone modem access to the libraries' computers, which are themselves connected to the Internet. Increasingly, patrons now use library services and resources without ever physically entering the library itself. Libraries typically provide such direct or modem access at no cost to the individual user.

17. Individuals can also access the Internet by patronizing an increasing number of storefront "computer coffee shops," where customers -- while they drink their coffee -- can use computers provided by the shop to access the Internet. Such Internet access is typically provided by the shop for a small hourly fee.

18. Individuals can also access the Internet through commercial and non-commercial "Internet service providers" that typically offer modem telephone access to a computer or computer network linked to the Internet. Many such providers -- including the members of plaintiff Commercial Internet Exchange Association -- are commercial entities offering Internet access for a monthly or hourly fee. Some Internet service providers, however, are non-profit organizations that offer free or very low cost access to the Internet. For example, the International Internet Association offers free modem access to the Internet upon request. Also, a number of trade or other non-profit associations offer Internet access as a service to members.

19. Another common way for individuals to access the Internet is through one of the major national commercial "online services" such as America Online, CompuServe, the Microsoft Network, or Prodigy. These online services offer nationwide computer networks (so that subscribers can dial-in to a local telephone number), and the services provide extensive and well organized content within their own proprietary computer networks. In addition to allowing access to the extensive content available within each online service, the services also allow subscribers to link to the much larger resources of the Internet. Full access to the online service (including access to the Internet) can be obtained for modest monthly or hourly fees. The major commercial online services have almost twelve million individual subscribers across the United States.

20. In addition to using the national commercial online services, individuals can also access the Internet using some (but not all) of the thousands of local dial-in computer services, often called "bulletin board systems" or "BBSs." With an investment of as little as $2,000.00 and the cost of a telephone line, individuals, non-profit organizations, advocacy groups, and businesses can offer their own dial-in computer "bulletin board" service where friends, members, subscribers, or customers can exchange ideas and information. BBSs range from single computers with only one telephone line into the computer (allowing only

one user at a time), to single computers with many telephone lines into the computer (allowing multiple simultaneous users), to multiple linked computers each servicing multiple dial-in telephone lines (allowing multiple simultaneous users). Some (but not all) of these BBS systems offer direct or indirect links to the Internet. Some BBS systems charge users a nominal fee for access, while many others are free to the individual users.

21. Although commercial access to the Internet is growing rapidly, many users of the Internet -- such as college students and staff -- do not individually pay for access (except to the extent, for example, that the cost of computer services is a component of college tuition). These and other Internet users can access the Internet without paying for such access with a credit card or other form of payment.

Methods to Communicate Over the Internet

22. Once one has access to the Internet, there are a wide variety of different methods of communication and information exchange over the network. These many methods of communication and information retrieval are constantly evolving and are therefore difficult to categorize concisely. The most common methods of communications on the Internet (as well as within the major online services) can be roughly grouped into six categories:

(1) one-to-one messaging (such as "e-mail"),

(2) one-to-many messaging (such as "listserv"),

(3) distributed message databases (such as "USENET newsgroups"),

(4) real time communication (such as "Internet Relay Chat"),

(5) real time remote computer utilization (such as "telnet"), and

(6) remote information retrieval (such as "ftp," "gopher," and the "World Wide Web").

Most of these methods of communication can be used to transmit text, data, computer programs, sound, visual images (i.e., pictures), and moving video images.

23. One-to-one messaging. One method of communication on the Internet is via electronic mail, or "e-mail," comparable in principle to sending a first class letter. One can address and transmit a message to one or more other people. E-mail on the Internet is not routed through a central control point, and can take many and varying paths to the recipients. Unlike postal mail, simple e-mail generally is not "sealed" or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted).

24. One-to-many messaging. The Internet also contains automatic mailing list services (such as "listservs"), [also referred to by witnesses as "mail exploders"] that allow communications about particular subjects of interest to a group of people. For example, people can subscribe to a "listserv" mailing list on a particular topic of interest to them. The subscriber can submit messages on the topic to the listserv that are forwarded (via e-mail), either automatically or through a human moderator overseeing the listserv, to anyone who has subscribed to the mailing list. A recipient of such a message can reply to the message and have the reply also distributed to everyone on the mailing list. This service provides the capability to keep abreast of developments or events in a particular subject area. Most listserv-type mailing lists automatically forward all incoming messages to all mailing list

subscribers. There are thousands of such mailing list services on the Internet, collectively with hundreds of thousands of subscribers. Users of "open" listservs typically can add or remove their names from the mailing list automatically, with no direct human involvement. Listservs may also be "closed," i.e., only allowing for one's acceptance into the listserv by a human moderator.

25. Distributed message databases. Similar in function to listservs -- but quite different in how communications are transmitted -- are distributed message databases such as "USENET newsgroups." User-sponsored newsgroups are among the most popular and widespread applications of Internet services, and cover all imaginable topics of interest to users. Like listservs, newsgroups are open discussions and exchanges on particular topics. Users, however, need not subscribe to the discussion mailing list in advance, but can instead access the database at any time. Some USENET newsgroups are "moderated" but most are open access. For the moderated newsgroups,(10) all messages to the newsgroup are forwarded to one person who can screen them for relevance to the topics under discussion. USENET newsgroups are disseminated using ad hoc, peer to peer connections between approximately 200,000 computers (called USENET "servers") around the world. For unmoderated newsgroups, when an individual user with access to a USENET server posts a message to a newsgroup, the message is automatically forwarded to all adjacent USENET servers that furnish access to the newsgroup, and it is then propagated to the servers adjacent to those servers, etc. The messages are temporarily stored on each receiving server, where they are available for review and response by individual users. The messages are automatically and periodically purged from each system after a time to make room for new messages. Responses to messages, like the original messages, are automatically distributed to all other computers receiving the newsgroup or forwarded to a moderator in the case of a moderated newsgroup. The dissemination of messages to USENET servers around the world is an automated process that does not require direct human intervention or review.

26. There are newsgroups on more than fifteen thousand different subjects. In 1994, approximately 70,000 messages were posted to newsgroups each day, and those messages were distributed to the approximately 190,000 computers or computer networks that participate in the USENET newsgroup system. Once the messages reach the approximately 190,000 receiving computers or computer networks, they are available to individual users of those computers or computer networks. Collectively, almost 100,000 new messages (or "articles") are posted to newsgroups each day.

27. Real time communication. In addition to transmitting messages that can be later read or accessed, individuals on the Internet can engage in an immediate dialog, in "real time", with other people on the Internet. In its simplest forms, "talk" allows one-to-one communications and "Internet Relay Chat" (or IRC) allows two or more to type messages to each other that almost immediately appear on the others' computer screens. IRC is analogous to a telephone party line, using a computer and keyboard rather than a telephone. With IRC, however, at any one time there are thousands of different party lines available, in which collectively tens of thousands of users are engaging in conversations on a huge range of subjects. Moreover, one can create a new party line to discuss a different topic at any time. Some IRC conversations are "moderated" or include "channel operators."

28. In addition, commercial online services such as America Online, CompuServe, the Microsoft Network, and Prodigy have their own "chat" systems allowing their members to converse.

29. Real time remote computer utilization. Another method to use information on the Internet is to access and control remote computers in "real time" using "telnet." For example, using telnet, a researcher at a university would be able to use the computing power of a supercomputer located at a different university. A student can use telnet to connect to a remote library to access the library's online card catalog program.

30. Remote information retrieval. The final major category of communication may be the most well known use of the Internet -- the search for and retrieval of information located on remote computers. There are three primary methods to locate and retrieve information on the Internet.

31. A simple method uses "ftp" (or file transfer protocol) to list the names of computer files available on a remote computer, and to transfer one or more of those files to an individual's local computer.

32. Another approach uses a program and format named "gopher" to guide an individual's search through the resources available on a remote computer.

The World Wide Web

33. A third approach, and fast becoming the most well-known on the Internet, is the "World Wide Web." The Web utilizes a "hypertext" formatting language called hypertext markup language (HTML), and programs that "browse" the Web can display HTML documents containing text, images, sound, animation and moving video. Any HTML document can include links to other types of information or resources, so that while viewing an HTML document that, for example, describes resources available on the Internet, one can "click" using a computer mouse on the description of the resource and be immediately connected to the resource itself. Such "hyperlinks" allow information to be accessed and organized in very flexible ways, and allow people to locate and efficiently view related information even if the information is stored on numerous computers all around the world.

34. Purpose. The World Wide Web (W3C) was created to serve as the platform for a global, online store of knowledge, containing information from a diversity of sources and accessible to Internet users around the world. Though information on the Web is contained in individual computers, the fact that each of these computers is connected to the Internet through W3C protocols allows all of the information to become part of a single body of knowledge. It is currently the most advanced information system developed on the Internet, and embraces within its data model most information in previous networked information systems such as ftp, gopher, wais, and Usenet.

35. History. W3C was originally developed at CERN, the European Particle Physics Laboratory, and was initially used to allow information sharing within internationally dispersed teams of researchers and engineers. Originally aimed at the High Energy Physics community, it has spread to other areas and attracted much interest in user support, resource recovery, and many other areas which depend on collaborative and information sharing. The Web has extended beyond the scientific and academic community to include communications by individuals, non-profit organizations, and businesses.

36. Basic Operation. The World Wide Web is a series of documents stored in different computers all over the Internet. Documents contain information stored in a variety of formats, including text, still images, sounds, and video. An essential element of the Web is that any document has an address (rather like a telephone number). Most Web documents contain "links." These are short sections of text or image which refer to another document. Typically the linked text is blue or underlined when displayed, and when selected by the user, the referenced document is automatically displayed, wherever in the world it actually is stored. Links for example are used to lead from overview documents to more detailed documents, from tables of contents to particular pages, but also as cross-references, footnotes, and new forms of information structure.

37. Many organizations now have "home pages" on the Web. These are documents which provide a set of links designed to represent the organization, and through links from the home page, guide the user directly or indirectly to information about or relevant to that

organization.

38. As an example of the use of links, if these Findings were to be put on a World Wide Web site, its home page might contain links such as those:

- THE NATURE OF CYBERSPACE
- CREATION OF THE INTERNET AND THE DEVELOPMENT OF CYBERSPACE
- HOW PEOPLE ACCESS THE INTERNET
- METHODS TO COMMUNICATE OVER THE INTERNET

39. Each of these links takes the user of the site from the beginning of the Findings to the appropriate section within this Adjudication. Links may also take the user from the original Web site to another Web site on another computer connected to the Internet. These links from one computer to another, from one document to another across the Internet, are what unify the Web into a single body of knowledge, and what makes the Web unique. The Web was designed with a maximum target time to follow a link of one tenth of a second.

40. Publishing. The World Wide Web exists fundamentally as a platform through which people and organizations can communicate through shared information. When information is made available, it is said to be "published" on the Web. Publishing on the Web simply requires that the "publisher" has a computer connected to the Internet and that the computer is running W3C server software. The computer can be as simple as a small personal computer costing less than $1500 dollars or as complex as a multi-million dollar mainframe computer. Many Web publishers choose instead to lease disk storage space from someone else who has the necessary computer facilities, eliminating the need for actually owning any equipment oneself.

41. The Web, as a universe of network accessible information, contains a variety of documents prepared with quite varying degrees of care, from the hastily typed idea, to the professionally executed corporate profile. The power of the Web stems from the ability of a link to point to any document, regardless of its status or physical location.

42. Information to be published on the Web must also be formatted according to the rules of the Web standards. These standardized formats assure that all Web users who want to read the material will be able to view it. Web standards are sophisticated and flexible enough that they have grown to meet the publishing needs of many large corporations, banks, brokerage houses, newspapers and magazines which now publish "online" editions of their material, as well as government agencies, and even courts, which use the Web to disseminate information to the public. At the same time, Web publishing is simple enough that thousands of individual users and small community organizations are using the Web to publish their own personal "home pages," the equivalent of individualized newsletters about that person or organization, which are available to everyone on the Web.

43. Web publishers have a choice to make their Web sites open to the general pool of all Internet users, or close them, thus making the information accessible only to those with advance authorization. Many publishers choose to keep their sites open to all in order to give their information the widest potential audience. In the event that the publishers choose to maintain restrictions on access, this may be accomplished by assigning specific user names and passwords as a prerequisite to access to the site. Or, in the case of Web sites maintained for internal use of one organization, access will only be allowed from other computers within that organization's local network.(11)

44. Searching the Web. A variety of systems have developed that allow users of the Web to search particular information among all of the public sites that are part of the Web. Services such as Yahoo, Magellan, Altavista, Webcrawler, and Lycos are all services known as "search engines" which allow users to search for Web sites that contain certain categories of information, or to search for key words. For example, a Web user looking for the text of

Supreme Court opinions would type the words "Supreme Court" into a search engine, and then be presented with a list of World Wide Web sites that contain Supreme Court information. This list would actually be a series of links to those sites. Having searched out a number of sites that might contain the desired information, the user would then follow individual links, browsing through the information on each site, until the desired material is found. For many content providers on the Web, the ability to be found by these search engines is very important.

45. Common standards. The Web links together disparate information on an ever-growing number of Internet-linked computers by setting common information storage formats (HTML) and a common language for the exchange of Web documents (HTTP). Although the information itself may be in many different formats, and stored on computers which are not otherwise compatible, the basic Web standards provide a basic set of standards which allow communication and exchange of information. Despite the fact that many types of computers are used on the Web, and the fact that many of these machines are otherwise incompatible, those who "publish" information on the Web are able to communicate with those who seek to access information with little difficulty because of these basic technical standards.

46. A distributed system with no centralized control. Running on tens of thousands of individual computers on the Internet, the Web is what is known as a distributed system. The Web was designed so that organizations with computers containing information can become part of the Web simply by attaching their computers to the Internet and running appropriate World Wide Web software. No single organization controls any membership in the Web, nor is there any single centralized point from which individual Web sites or services can be blocked from the Web. From a user's perspective, it may appear to be a single, integrated system, but in reality it has no centralized control point.

47. Contrast to closed databases. The Web's open, distributed, decentralized nature stands in sharp contrast to most information systems that have come before it. Private information services such as Westlaw, Lexis/Nexis, and Dialog, have contained large storehouses of knowledge, and can be accessed from the Internet with the appropriate passwords and access software. However, these databases are not linked together into a single whole, as is the World Wide Web.

48. Success of the Web in research, education, and political activities. The World Wide Web has become so popular because of its open, distributed, and easy-to-use nature. Rather than requiring those who seek information to purchase new software or hardware, and to learn a new kind of system for each new database of information they seek to access, the Web environment makes it easy for users to jump from one set of information to another. By the same token, the open nature of the Web makes it easy for publishers to reach their intended audiences without having to know in advance what kind of computer each potential reader has, and what kind of software they will be using.

Restricting Access to Unwanted On-Line Material(12)

PICS

49. With the rapid growth of the Internet, the increasing popularity of the Web, and the existence of material online that some parents may consider inappropriate for their children, various entities have begun to build systems intended to enable parents to control the material which comes into their homes and may be accessible to their children. The World Wide Web Consortium launched the PICS ("Platform for Internet Content Selection")

program in order to develop technical standards that would support parents' ability to filter and screen material that their children see on the Web.

50. The Consortium intends that PICS will provide the ability for third parties, as well as individual content providers, to rate content on the Internet in a variety of ways. When fully implemented, PICS-compatible World Wide Web browsers, Usenet News Group readers, and other Internet applications, will provide parents the ability to choose from a variety of rating services, or a combination of services.

51. PICS working group [PICS-WG] participants include many of the major online services providers, commercial internet access providers, hardware and software companies, major internet content providers, and consumer organizations. Among active participants in the PICS effort are:

Adobe Systems, Inc.

Apple Computer

America Online

AT&T

Center for Democracy and Technology

CompuServe

Delphi Internet Services

Digital Equipment Corporation

IBM

First floor

First Virtual Holdings Incorporated

France Telecom

FTP Software

Industrial Technology Research Institute of Taiwan

Information Technology Association of America

Institut National de Recherche en Informatique et en Automatique (INRIA)

Interactive Services Association

MCI

Microsoft

MIT/LCS/World Wide Web Consortium

NCD

NEC

Netscape Communications Corporation

NewView

O'Reilly and Associates

Open Market

Prodigy Services Company

Progressive Networks

Providence Systems/Parental Guidance

Recreational Software Advisory Council

SafeSurf

SoftQuad, Inc.

Songline Studios

Spyglass

SurfWatch Software

Telequip Corp.

Time Warner Pathfinder

Viacom Nickelodeon(13)

52. Membership in the PICS-WG includes a broad cross-section of companies from the computer, communications, and content industries, as well as trade associations and public interest groups. PICS technical specifications have been agreed to, allowing the Internet community to begin to deploy products and services based on the PICS-standards.

53. Until a majority of sites on the Internet have been rated by a PICS rating service, PICS will initially function as a "positive" ratings system in which only those sites that have been rated will be displayed using PICS compatible software. In other words, PICS will initially function as a site inclusion list rather than a site exclusion list. The default configuration for a PICS compatible Internet application will be to block access to all sites which have not been rated by a PICS rating service, while allowing access to sites which have a PICS rating for appropriate content.(14)

Software

54. For over a year, various companies have marketed stand alone software that is intended to enable parents and other adults to limit the Internet access of children. Examples of such software include: Cyber Patrol, CYBERsitter, The Internet Filter, Net Nanny, Parental Guidance, SurfWatch, Netscape Proxy Server, and WebTrack. The market for this type of software is growing, and there is increasing competition among software providers to provide products.

Cyber Patrol

55. As more people, particularly children, began to use the Internet, Microsystems Software, Inc. decided to develop and market Internet software intended to empower parents to exercise individual choice over what material their children could access. Microsystems' stated intent is to develop a product which would give parents comfort that their children can reap the benefits of the Internet while shielding them from objectionable or otherwise inappropriate materials based on the parents' own particular tastes and values. Microsystems' product, Cyber Patrol, was developed to address this need.

56. Cyber Patrol was first introduced in August 1995, and is currently available in Windows and Macintosh versions. Cyber Patrol works with both direct Internet Access providers (ISPs, e.g., Netcom, PSI, UUnet), and Commercial Online Service Providers (e.g., America Online, Compuserv, Prodigy, Microsoft). Cyber Patrol is also compatible with all major World Wide Web browsers on the market (e.g., Netscape, Navigator, Mosaic, Prodigy's Legacy and Skimmer browsers, America Online, Netcom's NetCruiser, etc.). Cyber Patrol was the first parental empowerment application to be compatible with the PICS standard. In February of 1996, Microsystems put the first PICS ratings server on the Internet.

57. The CyberNOT list contains approximately 7000 sites in twelve categories. The software is designed to enable parents to selectively block access to any or all of the twelve CyberNOT categories simply by checking boxes in the Cyber Patrol Headquarters (the Cyber Patrol program manager). These categories are:

> Violence/Profanity: Extreme cruelty, physical or emotional acts against any animal or person which are primarily intended to hurt or inflict pain. Obscene words, phrases, and profanity defined as text that uses George Carlin's seven censored words more often than once every fifty messages or pages.
>
> Partial Nudity: Full or partial exposure of the human anatomy except when exposing genitalia.
>
> Nudity: Any exposure of the human genitalia.
>
> Sexual Acts (graphic or text): Pictures or text exposing anyone or anything involved in explicit sexual acts and lewd and lascivious behavior, including masturbation, copulation, pedophilia, intimacy and involving nude or partially nude people in heterosexual, bisexual, lesbian or homosexual encounters. Also includes phone sex ads, dating services, adult personals, CD-ROM and videos.
>
> Gross Depictions (graphic or text): Pictures or descriptive text of anyone or anything which are crudely vulgar, deficient in civility or behavior, or showing scatological impropriety. Includes such depictions as maiming, bloody figures, indecent depiction of bodily functions.
>
> Racism/Ethnic Impropriety: Prejudice or discrimination against any race or ethnic culture. Ethnic or racist jokes and slurs. Any text that elevates one race over another.
>
> Satanic/Cult: Worship of the devil; affinity for evil, wickedness. Sects or groups that potentially coerce individuals to grow, and keep, membership.
>
> Drugs/Drug Culture: Topics dealing with the use of illegal drugs for entertainment. This would exclude current illegal drugs used for medicinal purposes (e.g., drugs used to treat victims of AIDS). Includes substances used for other than their primary purpose to alter the individual's state of mind such

as glue sniffing.

Militant/Extremist: Extremely aggressive and combative behaviors, radicalism, advocacy of extreme political measures. Topics include extreme political groups that advocate violence as a means to achieve their goal.

Gambling: Of or relating to lotteries, casinos, betting, numbers games, on-line sports or financial betting including non-monetary dares.

Questionable/Illegal: Material or activities of a dubious nature which may be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, software piracy, and copyright infringement.

Alcohol, Beer & Wine: Material pertaining to the sale or consumption of alcoholic beverages. Also includes sites and information relating to tobacco products.

58. Microsystems employs people to search the Internet for sites containing material in these categories. Since new sites are constantly coming online, Microsystems updates the CyberNOT list on a weekly basis. Once installed on the home PC, the copy of Cyber Patrol receives automatic updates to the CyberNOT list over the Internet every seven days.

59. In February of 1996, Microsystems signed a licensing arrangement with CompuServe, one of the leading commercial online services with over 4.3 million subscribers. CompuServe provides Cyber Patrol free of charge to its subscribers. Microsystems the same month signed a licensing arrangement with Prodigy, another leading commercial online service with over 1.4 million subscribers. Prodigy will provide Cyber Patrol free of charge of its subscribers.

60. Cyber Patrol is also available directly from Microsystems for $49.95, which includes a six month subscription to the CyberNOT blocked sites list (updated automatically once every seven days). After six months, parents can receive six months of additional updates for $19.95, or twelve months for $29.95. Cyber Patrol Home Edition, a limited version of Cyber Patrol, is available free of charge on the Internet. To obtain either version, parents download a seven day demonstration version of the full Cyber Patrol product from the Microsystems Internet World Wide Web Server. At the end of the seven day trial period, users are offered the opportunity to purchase the complete version of Cyber Patrol or provide Microsystems some basic demographic information in exchange for unlimited use of the Home Edition. The demographic information is used for marketing and research purposes. Since January of 1996, over 10,000 demonstration copies of Cyber Patrol have been downloaded from Microsystems' Web site.

61. Cyber Patrol is also available from Retail outlets as NetBlocker Plus. NetBlocker Plus sells for $19.95, which includes five weeks of updates to the CyberNOT list.

62. Microsystems also sells Cyber Patrol into a growing market in schools. As more classrooms become connected to the Internet, many teachers want to ensure that their students can receive the benefit of the Internet without encountering material they deem educationally inappropriate.

63. Microsystems is working with the Recreational Software Advisory Council (RSAC), a non-profit corporation which developed rating systems for video games, to implement the RSAC rating system for the Internet.

64. The next release of Cyber Patrol, expected in second quarter of this year, will give parents the ability to use any PICS rating service, including the RSAC rating service, in addition to the Microsystems CyberNOT list.

65. In order to speed the implementation of PICS and encourage the development of PICS-compatible Internet applications, Microsystems maintains a server on the Internet which contains its CyberNOT list. The server provides software developers with access to a PICS rating service, and allows software developers to test their products' ability to interpret standard PICS labels. Microsystems is also offering its PICS client test program for Windows free of charge. The client program can be used by developers of PICS rating services to test their services and products.

SurfWatch

66. Another software product, SurfWatch, is also designed to allow parents and other concerned users to filter unwanted material on the Internet. SurfWatch is available for both Apple Macintosh, Microsoft Windows, and Microsoft Windows 95 Operating Systems, and works with direct Internet Access Providers (e.g., Netcom, PSI, UUnet, AT&T, and more than 1000 other Internet Service Providers).

67. The suggested retail price of SurfWatch Software is $49.95, with a street price of between $20.00 and $25.00. The product is also available as part of CompuServe/Spry Inc.'s Internet in a Box for Kids, which includes access to Spry's Kids only Internet service and a copy of SurfWatch. Internet in a Box for Kids retails for approximately $30.00. The subscription service, which updates the SurfWatch blocked site list automatically with new sites each month, is available for $5.95 per month or $60.00 per year. The subscription is included as part of the Internet in a Box for Kids program, and is also provided as a low-cost option from Internet Service Providers.

68. SurfWatch is available at over 12,000 retail locations, including National stores such as Comp USA, Egghead Software, Computer City, and several national mail order outlets. SurfWatch can also be ordered directly from its own site on the World Wide Web, and through the Internet Shopping Network.

69. Plaintiffs America Online (AOL), Microsoft Network, and Prodigy all offer parental control options free of charge to their members. AOL has established an online area designed specifically for children. The "Kids Only" parental control feature allows parents to establish an AOL account for their children that accesses only the Kids Only channel on America Online.(15)

70. AOL plans to incorporate PICS-compatible capability into its standard Web browser software, and to make available to subscribers other PICS-compatible Web browsers, such as the Netscape software.

71. Plaintiffs CompuServe and Prodigy give their subscribers the option of blocking all access to the Internet, or to particular media within their proprietary online content, such as bulletin boards and chat rooms.

72. Although parental control software currently can screen for certain suggestive words or for known sexually explicit sites, it cannot now screen for sexually explicit images unaccompanied by suggestive text unless those who configure the software are aware of the particular site.

73. Despite its limitations, currently available user-based software suggests that a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be widely available.

Content on the Internet

74. The types of content now on the Internet defy easy classification. The entire card catalogue of the Carnegie Library is on-line, together with journals, journal abstracts, popular magazines, and titles of compact discs. The director of the Carnegie Library, Robert Croneberger, testified that on-line services are the emerging trend in libraries generally. Plaintiff Hotwired Ventures LLC organizes its Web site into information regarding travel, news and commentary, arts and entertainment, politics, and types of drinks. Plaintiff America Online, Inc., not only creates chat rooms for a broad variety of topics, but also allows members to create their own chat rooms to suit their own tastes. The ACLU uses an America Online chat room as an unmoderated forum for people to debate civil liberties issues. Plaintiffs' expert, Scott Bradner,(16) estimated that 15,000 newsgroups exist today, and he described his own interest in a newsgroup devoted solely to Formula 1 racing cars. America Online makes 15,000 bulletin boards available to its subscribers, who post between 200,000 and 250,000 messages each day. Another plaintiffs' expert, Harold Rheingold, participates in "virtual communities" that simulate social interaction. It is no exaggeration to conclude that the content on the Internet is as diverse as human thought.

75. The Internet is not exclusively, or even primarily, a means of commercial communication. Many commercial entities maintain Web sites to inform potential consumers about their goods and services, or to solicit purchases, but many other Web sites exist solely for the dissemination of non-commercial information. The other forms of Internet communication -- e-mail, bulletin boards, newsgroups, and chat rooms -- frequently have non-commercial goals. For the economic and technical reasons set forth in the following paragraphs, the Internet is an especially attractive means for not-for-profit entities or public interest groups to reach their desired audiences. There are examples in the parties' stipulation of some of the non-commercial uses that the Internet serves. Plaintiff Human Rights Watch, Inc., offers information on its Internet site regarding reported human rights abuses around the world. Plaintiff National Writers Union provides a forum for writers on issues of concern to them. Plaintiff Stop Prisoner Rape, Inc., posts text, graphics, and statistics regarding the incidence and prevention of rape in prisons. Plaintiff Critical Path AIDS Project, Inc., offers information on safer sex, the transmission of HIV, and the treatment of AIDS.

76. Such diversity of content on the Internet is possible because the Internet provides an easy and inexpensive way for a speaker to reach a large audience, potentially of millions. The start-up and operating costs entailed by communication on the Internet are significantly lower than those associated with use of other forms of mass communication, such as television, radio, newspapers, and magazines. This enables operation of their own Web sites not only by large companies, such as Microsoft and Time Warner, but also by small, not-for-profit groups, such as Stop Prisoner Rape and Critical Path AIDS Project. The Government's expert, Dr. Dan R. Olsen,(17) agreed that creation of a Web site would cost between $1,000 and $15,000, with monthly operating costs depending on one's goals and the Web site's traffic. Commercial online services such as America Online allow subscribers to create Web pages free of charge. Any Internet user can communicate by posting a message to one of the thousands of newsgroups and bulletin boards or by engaging in an on-line "chat", and thereby reach an audience worldwide that shares an interest in a particular topic.

77. The ease of communication through the Internet is facilitated by the use of hypertext markup language (HTML), which allows for the creation of "hyperlinks" or "links". HTML enables a user to jump from one source to other related sources by clicking on the link. A link might take the user from Web site to Web site, or to other files within a particular Web site. Similarly, by typing a request into a search engine, a user can retrieve many different sources of content related to the search that the creators of the engine have collected.

78. Because of the technology underlying the Internet, the statutory term "content provider,"(18) which is equivalent to the traditional "speaker," may actually be a hybrid of speakers. Through the use of HTML, for example, Critical Path and Stop Prisoner Rape link their Web sites to several related databases, and a user can immediately jump from the home pages of these organizations to the related databases simply by clicking on a link. America Online creates chat rooms for particular discussions but also allows subscribers to create their own chat rooms. Similarly, a newsgroup gathers postings on a particular topic and distributes them to the newsgroup's subscribers. Users of the Carnegie Library can read on-line versions of Vanity Fair and Playboy, and America Online's subscribers can peruse the New York Times, Boating, and other periodicals. Critical Path, Stop Prisoner Rape, America Online and the Carnegie Library all make available content of other speakers over whom they have little or no editorial control.

79. Because of the different forms of Internet communication, a user of the Internet may speak or listen interchangeably, blurring the distinction between "speakers" and "listeners" on the Internet. Chat rooms, e-mail, and newsgroups are interactive forms of communication, providing the user with the opportunity both to speak and to listen.

80. It follows that unlike traditional media, the barriers to entry as a speaker on the Internet do not differ significantly from the barriers to entry as a listener. Once one has entered cyberspace, one may engage in the dialogue that occurs there. In the argot of the medium, the receiver can and does become the content provider, and vice-versa.

81. The Internet is therefore a unique and wholly new medium of worldwide human communication.

Sexually Explicit Material On the Internet

82. The parties agree that sexually explicit material exists on the Internet. Such material includes text, pictures, and chat, and includes bulletin boards, newsgroups, and the other forms of Internet communication, and extends from the modestly titillating to the hardest-core.

83. There is no evidence that sexually-oriented material is the primary type of content on this new medium. Purveyors of such material take advantage of the same ease of access available to all users of the Internet, including establishment of a Web site.

84. Sexually explicit material is created, named, and posted in the same manner as material that is not sexually explicit. It is possible that a search engine can accidentally retrieve material of a sexual nature through an imprecise search, as demonstrated at the hearing. Imprecise searches may also retrieve irrelevant material that is not of a sexual nature. The accidental retrieval of sexually explicit material is one manifestation of the larger phenomenon of irrelevant search results.

85. Once a provider posts content on the Internet, it is available to all other Internet users worldwide. Similarly, once a user posts a message to a newsgroup or bulletin board, that message becomes available to all subscribers to that newsgroup or bulletin board. For example, when the UCR/California Museum of Photography posts to its Web site nudes by Edward Weston and Robert Mapplethorpe to announce that its new exhibit will travel to Baltimore and New York City, those images are available not only in Los Angeles, Baltimore, and New York City, but also in Cincinnati, Mobile, or Beijing -- wherever Internet users live. Similarly, the safer sex instructions that Critical Path posts to its Web site, written in street language so that the teenage receiver can understand them, are available not just in Philadelphia, but also in Provo and Prague. A chat room organized by the ACLU to discuss the United States Supreme Court's decision in FCC v. Pacifica Foundation would transmit George Carlin's seven dirty words to anyone who enters.

Messages posted to a newsgroup dedicated to the Oklahoma City bombing travel to all subscribers to that newsgroup.

86. Once a provider posts its content on the Internet, it cannot prevent that content from entering any community. Unlike the newspaper, broadcast station, or cable system, Internet technology necessarily gives a speaker a potential worldwide audience. Because the Internet is a network of networks (as described above in Findings 1 through 4), any network connected to the Internet has the capacity to send and receive information to any other network. Hotwired Ventures, for example, cannot prevent its materials on mixology from entering communities that have no interest in that topic.

87. Demonstrations at the preliminary injunction hearings showed that it takes several steps to enter cyberspace. At the most fundamental level, a user must have access to a computer with the ability to reach the Internet (typically by way of a modem). A user must then direct the computer to connect with the access provider, enter a password, and enter the appropriate commands to find particular data. On the World Wide Web, a user must normally use a search engine or enter an appropriate address. Similarly, accessing newsgroups, bulletin boards, and chat rooms requires several steps.

88. Communications over the Internet do not "invade" an individual's home or appear on one's computer screen unbidden. Users seldom encounter content "by accident." A document's title or a description of the document will usually appear before the document itself takes the step needed to view it, and in many cases the user will receive detailed information about a site's content before he or she need take the step to access the document. Almost all sexually explicit images are preceded by warnings as to the content. Even the Government's witness, Agent Howard Schmidt, Director of the Air Force Office of Special Investigation, testified that the "odds are slim" that a user would come across a sexually explicit site by accident.

89. Evidence adduced at the hearing showed significant differences between Internet communications and communications received by radio or television. Although content on the Internet is just a few clicks of a mouse away from the user, the receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial. A child requires some sophistication and some ability to read to retrieve material and thereby to use the Internet unattended.

Obstacles to Age Verification on the Internet

90. There is no effective way to determine the identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups or chat rooms. An e-mail address provides no authoritative information about the addressee, who may use an e-mail "alias" or an anonymous remailer. There is also no universal or reliable listing of e-mail addresses and corresponding names or telephone numbers, and any such listing would be or rapidly become incomplete. For these reasons, there is no reliable way in many instances for a sender to know if the e-mail recipient is an adult or a minor. The difficulty of e-mail age verification is compounded for mail exploders such as listservs, which automatically send information to all e-mail addresses on a sender's list. Government expert Dr. Olsen agreed that no current technology could give a speaker assurance that only adults were listed in a particular mail exploder's mailing list.

91. Because of similar technological difficulties, individuals posting a message to a newsgroup or engaging in chat room discussions cannot ensure that all readers are adults, and Dr. Olsen agreed. Although some newsgroups are moderated, the moderator's control is limited to what is posted and the moderator cannot control who receives the messages.

92. The Government offered no evidence that there is a reliable way to ensure that recipients and participants in such fora can be screened for age. The Government presented no evidence demonstrating the feasibility of its suggestion that chat rooms, newsgroups and other fora that contain material deemed indecent could be effectively segregated to "adult" or "moderated" areas of cyberspace.

93. Even if it were technologically feasible to block minors' access to newsgroups and similar fora, there is no method by which the creators of newsgroups which contain discussions of art, politics or any other subject that could potentially elicit "indecent" contributions could limit the blocking of access by minors to such "indecent" material and still allow them access to the remaining content, even if the overwhelming majority of that content was not indecent.

94. Likewise, participants in MUDs (Multi-User Dungeons) and MUSEs (Multi-User Simulation Environments) do not know whether the other participants are adults or minors. Although MUDs and MUSEs require a password for permanent participants, they need not give their real name nor verify their age, and there is no current technology to enable the administrator of these fantasy worlds to know if the participant is an adult or a minor.

95. Unlike other forms of communication on the Internet, there is technology by which an operator of a World Wide Web server may interrogate a user of a Web site. An HTML document can include a fill-in-the-blank "form" to request information from a visitor to a Web site, and this information can be transmitted back to the Web server and be processed by a computer program, usually a Common Gateway Interface (cgi) script. The Web server could then grant or deny access to the information sought. The cgi script is the means by which a Web site can process a fill-in form and thereby screen visitors by requesting a credit card number or adult password.

96. Content providers who publish on the World Wide Web via one of the large commercial online services, such as America Online or CompuServe, could not use an online age verification system that requires cgi script because the server software of these online services available to subscribers cannot process cgi scripts. There is no method currently available for Web page publishers who lack access to cgi scripts to screen recipients online for age.

The Practicalities of the Proffered Defenses

Note: The Government contends the CDA makes available three potential defenses to all content providers on the Internet: credit card verification, adult verification by password or adult identification number, and "tagging".

Credit Card Verification

97. Verification(19) of a credit card number over the Internet is not now technically possible. Witnesses testified that neither Visa nor Mastercard considers the Internet to be sufficiently secure under the current technology to process transactions in that manner. Although users can and do purchase products over the Internet by transmitting their credit card number, the seller must then process the transaction with Visa or Mastercard off-line using phone lines in the traditional way. There was testimony by several witnesses that Visa and Mastercard are in the process of developing means of credit card verification over the Internet.

98. Verification by credit card, if and when operational, will remain economically and practically unavailable for many of the non-commercial plaintiffs in these actions. The

Government's expert "suspect[ed]" that verification agencies would decline to process a card unless it accompanied a commercial transaction. There was no evidence to the contrary.

99. There was evidence that the fee charged by verification agencies to process a card, whether for a purchase or not, will preclude use of the credit-card verification defense by many non-profit, non-commercial Web sites, and there was no evidence to the contrary. Plaintiffs' witness Patricia Nell Warren, an author whose free Web site allows users to purchase gay and lesbian literature, testified that she must pay $1 per verification to a verification agency. Her Web site can absorb this cost because it arises in connection with the sale of books available there.

100. Using credit card possession as a surrogate for age, and requiring use of a credit card to enter a site, would impose a significant economic cost on non-commercial entities. Critical Path, for example, received 3,300 hits daily from February 4 through March 4, 1996. If Critical Path must pay a fee every time a user initially enters its site, then, to provide free access to its non-commercial site, it would incur a monthly cost far beyond its modest resources. The ACLU's Barry Steinhardt testified that maintenance of a credit card verification system for all visitors to the ACLU's Web site would require it to shut down its Web site because the projected cost would exceed its budget.

101. Credit card verification would significantly delay the retrieval of information on the Internet. Dr. Olsen, the expert testifying for the Government, agreed that even "a minute is [an] absolutely unreasonable [delay] . . . [P]eople will not put up with a minute." Plaintiffs' expert Donna Hoffman similarly testified that excessive delay disrupts the "flow" on the Internet and stifles both "hedonistic" and "goal-directed" browsing.

102. Imposition of a credit card requirement would completely bar adults who do not have a credit card and lack the resources to obtain one from accessing any blocked material. At this time, credit card verification is effectively unavailable to a substantial number of Internet content providers as a potential defense to the CDA.

Adult Verification by Password

103. The Government offered very limited evidence regarding the operation of existing age verification systems, and the evidence offered was not based on personal knowledge. AdultCheck and Verify, existing systems which appear to be used for accessing commercial pornographic sites, charge users for their services. Dr. Olsen admitted that his knowledge of these services was derived primarily from reading the advertisements on their Web pages. He had not interviewed any employees of these entities, had not personally used these systems, had no idea how many people are registered with them, and could not testify to the reliability of their attempt at age verification.

104. At least some, if not almost all, non-commercial organizations, such as the ACLU, Stop Prisoner Rape or Critical Path AIDS Project, regard charging listeners to access their speech as contrary to their goals of making their materials available to a wide audience free of charge.

105. It would not be feasible for many non-commercial organizations to design their own adult access code screening systems because the administrative burden of creating and maintaining a screening system and the ongoing costs involved is beyond their reach. There was testimony that the costs would be prohibitive even for a commercial entity such as HotWired, the online version of Wired magazine.

106. There is evidence suggesting that adult users, particularly casual Web browsers, would be discouraged from retrieving information that required use of a credit card or password. Andrew Anker testified that HotWired has received many complaints from its members

about HotWired's registration system, which requires only that a member supply a name, e-mail address and self-created password. There is concern by commercial content providers that age verification requirements would decrease advertising and revenue because advertisers depend on a demonstration that the sites are widely available and frequently visited.

107. Even if credit card verification or adult password verification were implemented, the Government presented no testimony as to how such systems could ensure that the user of the password or credit card is in fact over 18. The burdens imposed by credit card verification and adult password verification systems make them effectively unavailable to a substantial number of Internet content providers.

The Government's "Tagging" Proposal

108. The feasibility and effectiveness of "tagging" to restrict children from accessing "indecent" speech, as proposed by the Government has not been established. "Tagging" would require content providers to label all of their "indecent" or "patently offensive" material by imbedding a string of characters, such as "XXX," in either the URL or HTML. If a user could install software on his or her computer to recognize the "XXX" tag, the user could screen out any content with that tag. Dr. Olsen proposed a "-L18" tag, an idea he developed for this hearing in response to Mr. Bradner's earlier testimony that certain tagging would not be feasible.

109. The parties appear to agree that it is technologically feasible -- "trivial", in the words of plaintiffs' expert -- to imbed tags in URLs and HTML, and the technology of tagging underlies both plaintiffs' PICS proposal and the Government's "-L18" proposal.

110. The Government's tagging proposal would require all content providers that post arguably "indecent" material to review all of their online content, a task that would be extremely burdensome for organizations that provide large amounts of material online which cannot afford to pay a large staff to review all of that material. The Carnegie Library would be required to hire numerous additional employees to review its on-line files at an extremely high cost to its limited budget. The cost and effort would be substantial for the Library and frequently prohibitive for others. Witness Kiroshi Kuromiya testified that it would be impossible for his organization, Critical Path, to review all of its material because it has only one full and one part-time employee.

111. The task of screening and tagging cannot be done simply by using software which screens for certain words, as Dr. Olsen acknowledged, and we find that determinations as to what is indecent require human judgment.

112. In lieu of reviewing each file individually, a content provider could tag its entire site but this would prevent minors from accessing much material that is not "indecent" under the CDA.

113. To be effective, a scheme such as the -L18 proposal would require a worldwide consensus among speakers to use the same tag to label "indecent" material. There is currently no such consensus, and no Internet speaker currently labels its speech with the -L18 code or with any other widely-recognized label.

114. Tagging also assumes the existence of software that recognizes the tags and takes appropriate action when it notes tagged speech. Neither commercial Web browsers nor user-based screening software is currently configured to block a -L18 code. Until such software exists, all speech on the Internet will continue to travel to whomever requests it, without hindrance. Labelling speech has no effect in itself on the transmission (or not) of that speech. Neither plaintiffs nor the Government suggest that tagging alone would shield

minors from speech or insulate a speaker from criminal liability under the CDA. It follows that all speech on any topic that is available to adults will also be available to children using the Internet (unless it is blocked by screening software running on the computer the child is using).

115. There is no way that a speaker can use current technology to know if a listener is using screening software.

116. Tags can not currently activate or deactivate themselves depending on the age or location of the receiver. Critical Path, which posts on-line safer sex instructions, would be unable to imbed tags that block its speech only in communities where it may be regarded as indecent. Critical Path, for example, must choose either to tag its site (blocking its speech in all communities) or not to tag, blocking its speech in none.

The Problems of Offshore Content and Caching

117. A large percentage, perhaps 40% or more, of content on the Internet originates outside the United States. At the hearing, a witness demonstrated how an Internet user could access a Web site of London (which presumably is on a server in England), and then link to other sites of interest in England. A user can sometimes discern from a URL that content is coming from overseas, since InterNIC allows a content provider to imbed a country code in a domain name.(20) Foreign content is otherwise indistinguishable from domestic content (as long as it is in English), since foreign speech is created, named, and posted in the same manner as domestic speech. There is no requirement that foreign speech contain a country code in its URL. It is undisputed that some foreign speech that travels over the Internet is sexually explicit.

118. The use of "caching" makes it difficult to determine whether the material originated from foreign or domestic sources. Because of the high cost of using the trans- Atlantic and trans-Pacific cables, and because the high demand on those cables leads to bottleneck delays, content is often "cached", or temporarily stored, on servers in the United States. Material from a foreign source in Europe can travel over the trans-Atlantic cable to the receiver in the United States, and pass through a domestic caching server which then stores a copy for subsequent retrieval. This domestic caching server, rather than the original foreign server, will send the material from the cache to the subsequent receivers, without placing a demand on the trans-oceanic cables. This shortcut effectively eliminates most of the distance for both the request and the information and, hence, most of the delay. The caching server discards the stored information according to its configuration (e.g., after a certain time or as the demand for the information diminishes). Caching therefore advances core Internet values: the cheap and speedy retrieval of information.

119. Caching is not merely an international phenomenon. Domestic content providers store popular domestic material on their caching servers to avoid the delay of successive searches for the same material and to decrease the demand on their Internet connection. America Online can cache the home page of the New York Times on its servers when a subscriber first requests it, so that subsequent subscribers who make the same request will receive the same home page, but from America Online's caching service rather than from the New York Times's server.(21)

120. Put simply, to follow the example in the prior paragraph, America Online has no control over the content that the New York Times posts to its Web site, and the New York Times has no control over America Online's distribution of that content from a caching server.

Anonymity

121. Anonymity is important to Internet users who seek to access sensitive information, such as users of the Critical Path AIDS Project's Web site, the users, particularly gay youth, of Queer Resources Directory, and users of Stop Prisoner Rape (SPR). Many members of SPR's mailing list have asked to remain anonymous due to the stigma of prisoner rape.

Plaintiffs' Choices Under the CDA

122. Many speakers who display arguably indecent content on the Internet must choose between silence and the risk of prosecution. The CDA's defenses -- credit card verification, adult access codes, and adult personal identification numbers -- are effectively unavailable for non-commercial, not-for-profit entities.

123. The plaintiffs in this action are businesses, libraries, non-commercial and not-for-profit organizations, and educational societies and consortia. Although some of the material that plaintiffs post online -- such as information regarding protection from AIDS, birth control or prison rape -- is sexually explicit and may be considered "indecent" or "patently offensive" in some communities, none of the plaintiffs is a commercial purveyor of what is commonly termed "pornography."

III.

CONCLUSIONS OF LAW

Plaintiffs have established a reasonable probability of eventual success in the litigation by demonstrating that §§ 223(a)(1)(B) and 223(a)(2) of the CDA are unconstitutional on their face to the extent that they reach indecency. Sections 223(d)(1) and 223(d)(2) of the CDA are unconstitutional on their face. Accordingly, plaintiffs have shown irreparable injury, no party has any interest in the enforcement of an unconstitutional law, and therefore the public interest will be served by granting the preliminary injunction. Elrod v. Burns, 427 U.S. 347, 373-74 (1976); Hohe v. Casey, 868 F.2d 69, 72 (3d Cir.), cert. denied, 493 U.S. 848 (1989); Acierno v. New Castle County, 40 F.3d 645, 653 (3d Cir. 1994). The motions for preliminary injunction will therefore be granted.

The views of the members of the Court in support of these conclusions follow.

SLOVITER, Chief Judge, Court of Appeals for the Third Circuit:

A.

Statutory Provisions

As noted in Part I, Introduction, the plaintiffs' motion for a preliminary injunction is confined to portions of two provisions of the Communications Decency Act of 1996, § 223(a) and § 223(d), which they contend violate their First Amendment free speech and Fifth Amendment due process rights. To facilitate reference, I set forth those provisions in full. Section 223(a), the "indecency" provision, subjects to criminal penalties of imprisonment of no more than two years or a fine or both anyone who:

BNA | TOP STORY | LIBRARY | FEEDBACK | SALES INFO

THE BUREAU OF NATIONAL AFFAIRS INC.

ELECTRONIC COMMERCE & LAW REPORT

MARKING 50 YEARS OF EMPLOYEE OWNERSHIP

Updated: 12/01/97 06:33 PM Eastern Standard Time

IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF PENNSYLVANIA

Cyber Promotions Inc.
vs.
America Online Inc.
C.A. NO. 96-2486

America Online Inc.
vs.
Cyber Promotions Inc.
C.A. NO. 96-5213

MEMORANDUM OPINION AND ORDER

Weiner, J.

November 4, 1996

These cases present the novel issue of whether, under the First Amendment to the United States Constitution, one private company has the unfettered right to send unsolicited e-mail advertisements to subscribers of another private online company over the Internet and whether the private online company has the right to block the e-mail advertisements from reaching its members. The question is important because while the Internet provides the opportunity to disseminate vast amounts of information, the Internet does not, at least at the present time, have any means to police the dissemination of that information. We therefore find that, in the absence of State action, the private online service has the right to prevent unsolicited e-mail solicitations from reaching its subscribers over the Internet.

The cases have their genesis in a letter dated January 26, 1996, in which American Online, Inc. ("AOL") advised Cyber Promotions, Inc. ("Cyber") that AOL was upset with Cyber's dissemination of unsolicited e-mail to AOL members over the Internet. AOL subsequently sent a number of "e-mail bombs" [1] to Cyber's Internet service providers ("ISP").

On March 26, 1996, Cyber filed Civil Action No. 96-2486 in this Court against AOL in response to AOL's "e-mail bombing" of Cyber's ISPs. The Complaint alleges that as a result of AOL's "e-mail bombing", two of Cyber's ISPs terminated their relationship with Cyber and a third ISP refused to enter into a contract with Cyber. The Complaint asserts a claim for violation of the Computer Fraud and Abuse Act, 18 U.S.C. Section 1030, as well as state law claims for intentional interference with contractual relations, tortious interference with prospective contractual relations and unfair competition. The Complaint seeks certain injunctive relief and damages.

On April 8, 1996, AOL filed a ten-count Complaint against Cyber in the United States District Court for the Eastern District of Virginia, alleging service and trade name infringement, service mark and trade

the Eastern District of Virginia, alleging service and trade name infringement, service mark and trade name dilution, false designation of origin, false advertising, unfair competition, violations of the Virginia Consumer Protection Act, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act and the Virginia Computer Crimes Act. AOL seeks various injunctive relief and damages.

On May 8, 1996, Cyber filed a First Amended Complaint in Civil Action No. 96-2486 in which it asserted the same four claims it asserted in its original Complaint and added a declaratory judgment claim (Count V). Cyber seeks, *inter alia*, a "declaration that [it] has the right to send to AOL members via the Internet unsolicited e-mail advertisements." Amended Complaint at p. 21. Cyber also asks the Court to "permanently enjoin[] AOL ... from ... directly or indirectly preventing AOL members from receiving [Cyber's] e-mail messages." *Id.*

On June 17, 1996, AOL filed a First Amended Complaint in the Virginia action in which it added claims for misappropriation, conversion, and unjust enrichment.

By Order dated July 24, 1996, the judge in the Eastern District of Virginia to whom AOL's action was assigned, transferred that action to this Court, finding that it arises from "the same nucleus of operative facts" as Cyber's action and that therefore "the two cases should be consolidated for trial." Upon transfer to this Court, AOL's action was assigned Civil Action No. 96-5213. The parties have agreed that the First Amended Complaint in that action will be treated as setting forth AOL's counterclaims in Civil Action No. 96-2486.

AOL has vehemently argued throughout the brief history of these suits that Cyber has no right to send literally millions of e-mail messages each day to AOL's Internet servers free of charge and resulting in the overload of the e-mail servers. Indeed, the court has received a plethora of letters from disgruntled AOL members who object to having to receive Cyber's unsolicited e-mail whenever they sign on to AOL despite repeated attempts to be removed from Cyber's lists. Cyber, on the other hand, has contended that without the right to send unsolicited e-mail to AOL members, it will go out of business.

Recognizing that Cyber's contention that it has the right to send unsolicited e-mail to AOL members over the Internet implicates the First Amendment and therefore is a threshold issue, the Court directed the parties to brief the following issue: Whether Cyber has a right under the First Amendment of the United States Constitution to send unsolicited e-mail to AOL members via the Internet and concomitantly whether AOL has the right under the First Amendment to block the e-mail sent by Cyber from reaching AOL members over the Internet. In response, AOL has filed a document entitled "Motion for Partial Summary Judgment of America Online, Inc. on First Amendment issues." Specifically, AOL seeks summary judgment on Cyber's declaratory judgment claim asserted in Count V of Cyber's First Amended Complaint. Cyber has filed a document entitled "Plaintiff's Memorandum in Support of its First Amendment Right to Send Internet E-Mail to Defendant's Members."

The Court also directed the parties to enter into a Stipulation of Facts solely for the purpose of resolving the First Amendment issue. Pursuant to the Court's directive, the parties have stipulated to the following facts:

1. Cyber is a corporation organized and existing under the laws of the Commonwealth of Pennsylvania, having a place of business at 1255 Passmore Street, 1st Floor, Philadelphia, Pennsylvania 19111.

2. AOL is a corporation organized and existing under the laws of the State of Delaware with its principal place of business at 22000 AOL Way, Dulles, Virginia 20166.

3. AOL was and is a private online company that has invested substantial sums of its own money in equipment, name, software and reputation. AOL is not owned in whole or in part by the government.

4. AOL is owned by shareholders, and its stock trades on the New York Stock Exchange.

6. AOL's members or subscribers pay prescribed fees for use of AOL resources, access to AOL and access and use of AOL's e-mail system and its connection to the Internet.

7. AOL's e-mail system operates through dedicated computers known as servers, which consist of computer hardware and software purchased, maintained and owned by AOL. AOL's computer servers have a finite, though expandable, capacity to handle e-mail. All Internet e-mail from non-AOL members to AOL customers or members and from AOL customers or members to non-AOL members requires the use of AOL's computer hardware and software in combination with the hardware and software of the Internet and the hardware and software of the non-AOL members.

9. There has been no government involvement in AOL's business decision to institute or reinstitute a block directed to Internet e-mail sent by Cyber to AOL members or subscribers.

10. Although the Internet is accessible to all persons with just a computer, a modem and a service provider, the constitu ent parts of the Internet (namely the computer hardware and software, servers, service providers and related items) are owned and managed by private entities and persons, corporations, educational institutions and government entities, who cooperate to allow their constituent parts to be interconnected by a vast network of phone lines.

11. In order for non-AOL members to send Internet e-mail to AOL members, non-AOL members must utilize a combination of their own hardware and software, the Internet and AOL's network.

12. To obtain its initial access to the Internet, AOL obtained an Internet address and domain name from IANA, a clearing house that routinely and ministerially assigns Internet addresses and domain names.

13. Cyber, an advertising agency incorporated in 1996, provides advertising services for companies and individuals wishing to advertise their products and services via e-mail.

14. Cyber sends its e-mail via the Internet to members of AOL, members of other commercial online services and other individuals with an Internet e-mail address.

15. AOL provides its subscribing members with one or more e-mail addresses so that members can exchange e-mail with one another and exchange e-mail (both sending and receiving) over the Internet with non-AOL members.

16. AOL has attached to its Memorandum of Law in Support of its Motion for Partial Summary Judgment on First Amendment Issues three sets of examples of e-mail messages sent by Cyber to AOL members. The first set (Tab 1) consists of a multi-page set of advertisements; the second set (Tab 2) consists of an exclusive or single-advertiser e-mail; and the third set (Tab 3) consists of a document called by Cyber an "e-mag." Under each tab are two examples, the first selected by AOL and the second selected by Cyber. The Court has reviewed all of the examples and notes that many of the ads include get-rich-quick ads, weight loss ads, health aid promises and even phone sex services.

17. To attract membership, AOL offers a variety of services, options, resources and support, including content-based services, access to stock quotes, children's entertainment, news, and the ability to send and receive Internet e-mail to and from non-AOL members.

In addition to the parties's Stipulation of Facts, it is necessary for resolution of the issue before us to relate some of the factual findings about the Internet itself made earlier this year by our court in *American Civil Liberties Union v. Reno*, 929 F.Supp. 824 (E.D. Pa. 1996). They are as follows:

18. "The Internet is ... a unique and wholly new medium of worldwide human

that party's case. *Celotex*, 477 U.S. at 323. If that evidence is, however, "`merely colorable' or is `not significantly probative,' summary judgment may be granted." *Equimark Commercial Finance Co. v. C.I.T. Financial Corp.* 812 F.2d 141, 144 (3d Cir. 1987) (quoting, in part, *Anderson*, 477 U.S. at 249-50).

In view of the parties' Stipulation of Facts and the prior factual findings of this Court in *ACLU v. Reno*, *supra*., the Court finds there are no genuine issues of material fact as to the First Amendment issue and that that issue is suitable for summary disposition.

In its Motion for Partial Summary Judgment, AOL contends that Cyber has no First Amendment right to send unsolicited e-mail to AOL members over the Internet because AOL is not a state actor, AOL's e-mail servers are not public fora in which Cyber has a right to speak, Cyber's right to use AOL's, service free of charge, does not substantially outweigh AOL's right to speak or not to speak, and that AOL's restrictions on mass e-mail solicitations are tailored to serve a substantial interest. Motion for Partial Summary Judgment at 6. Because we find AOL is not a state actor and none of its activities constitute state action, we need not consider AOL's remaining First Amendment contentions.

The First Amendment to the United States Constitution states that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press." The United States Supreme Court has recognized that "the constitutional guarantee of free speech is a guarantee only against abridgement by government, federal or state." *Hudgens v.NLRB*, 424 U.S. 507, 513 (1976). Only recently, the Supreme Court has stated that "the guarantees of free speech ... guard only against encroachment by the government and `erec[t] no shield against merely private conduct.'" *Hurley v. Irish-American Gay Group of Boston*, 115 S.Ct. 2338, 2344 (1995) (citation omitted).

In the case *sub judice*, the parties have stipulated that AOL is a *private* online company that is not owned in whole or part by the government. Stipulation of Facts at para. 3. (emphasis added). The parties have further stipulated that "AOL is not a government entity or political subdivision." *Id.* at para. 5. They have also stipulated that there has been no government involvement in AOL's business decision to institute or reinstitute a block directed to Internet e-mail sent by Cyber to AOL members or subscribers. *Id.* at para. 9.

Despite these stipulations, Cyber argues that AOL's conduct has the character of state action. As a general matter, private action can only be considered state action when "there is a sufficiently close nexus between the State and the challenged action of [the private entity] so that the action of the latter may be fairly treated as that of the State itself." *Blum v. Yaretsky*, 457 U.S. 991, 1004 (1982). Recently, our Court of Appeals observed that the Supreme Court appears to utilize three distinct tests in determining whether there has been state action. *Mark v. Borough of Hatboro*, 51 F.3d 1137, 1142 (3d Cir. 1995). First, we must consider whether "`the private entity has exercised powers that are traditionally the *exclusive* prerogative of the state.'" *Id.* (quoting *Blum v. Yaretsky*, 457 U.S. at 1004-05. (emphasis in *Mark*)). This test is known as the exclusive public function test. If the private entity does not exercise such powers, we must consider whether "`the private entity has acted with the help of or in concert with state officials.'" *Mark*, 51 F.3d at 1142 (quoting *McKeesport Hospital v. Accreditation Council for Graduate Medical Ed.*, 24 F.3d 519, 524 (3d Cir. 1994)). The final test is whether "`[t]he State has so far insinuated itself into a position of interdependence with ... [the acting party] that it must be recognized as a joint participant in the challenged activity.'" *Mark*, 51 F.3d at 1142 (quoting *Krynicky v. University of Pitts burgh*, 742 F.2d 94, 98 (3d Cir. 1984)).

With regard to the first test, AOL exercises absolutely no powers which are in any way the prerogative, let alone the *exclusive* prerogative, of the State. In *ACLU*, *supra*, this Court previously found that no single entity, including the State, administers the Internet. *ACLU*, 929 F.Supp. at 832. Rather, the Court found that the Internet is a "global Web of linked networks and computers" which exists and functions as the result of the desire of hundreds of thousands of computer operators and networks to use common data transfer data protocol to exchange communica tions and information. *Id.* In addition, "the constituent parts of the Internet ... are owned and managed by private entities and persons, corporations, educational institutions and government entities, who cooperate to allow their constituent parts to be interconnected by a vast network of phone lines." Stipulation of Facts at para. 10. As a result, tens of

interconnected by a vast network of phone lines." Stipulation of Facts at para. 10. As a result, tens of millions of people with access to the Internet can exchange information. AOL is merely one of many private online companies which allow its members access to the Internet through its e-mail system where they can exchange information with the general public. The State has absolutely no interest in, and does not regulate, this exchange of information between people, institutions, corporations and governments around the world.

Cyber argues, however, that "by providing Internet e-mail and acting as the sole conduit to its members' Internet e-mail boxes, AOL has opened up that part of its network and as such, has sufficiently devoted this domain for public use. This dedication of AOL's Internet e-mail accessway performs a public function in that it is open to the public, free of charge to any user, where public discourse, conversations and commercial transactions can and do take place." Cyber's Memorandum in Support of its First Amendment Right to Send Internet E-Mail to Defendant's Members at 13. Cyber therefore contends that AOL's Internet e-mail accessway is similar to the company town in *Marsh v. Alabama*, 326 U.S. 501 (1946), which the Supreme Court found performed a public function and therefore was a state actor.

In *Marsh*, a Jehovah's Witness was convicted of criminal trespass for distributing literature without a license on a sidewalk in a town owned by a private company. The Supreme Court found that since the private company owned the streets, sidewalks, and business block, paid the sheriff, privately owned and managed the sewage system, and owned the building where the United States post office was located, the company, in effect, operated as the municipal government of the town. *Marsh*, 326 U.S. at 502-03. "[T]he owner of the company town was performing the full spectrum of municipal powers and stood in the shoes of the State." *Lloyd Corp. V. Tanner*, 407 U.S. 551, 569 (1972). The Court observed that "[t]he more an owner, for his advantage, opens up his property for use by the public in general, the more do his rights become circumscribed by the statutory and constitutional rights of those who use it." *Marsh*, 326 U.S. at 506. As a result, the Court found state action in "the State['s] ... attempt[] to impose criminal punishment on appellant for undertaking to distribute religious literature in a company town ... " *Marsh*, 326 U.S. at 509. Our Court of Appeals has noted that "*Marsh* has been construed narrowly." *Cable Investments, Inc. v. Woolley*, 867 F.2d 151, 162 (3d Cir. 1989).[2]

By providing its members with access to the Internet through its e-mail system so that its members can exchange information with those members of the public who are also connected to the Internet, AOL is not exercising *any* of the municipal powers or public services traditionally exercised by the State as did the private company in *Marsh*. Although AOL has technically opened its e-mail system to the public by connecting with the Internet, AOL has not opened its property to the public by performing any municipal power or essential public service and, therefore, does not stand in the shoes of the State. *Marsh* is simply inapposite to the facts of the case *sub judice*.

Cyber also argues that AOL's Internet e-mail connection constitutes an exclusive public function because there are no alternative avenues of communication for Cyber to send its e-mail to AOL members. As support for this proposition, Cyber directs our attention to the decisions of the Supreme Court in *United States Postal Service v. Greenburgh Civic Assn's*, 453 U.S. 114 (1981); *Lloyd Corp v. Tanner*, 407 U.S. 551 (1972) and *Amalgamated Food Employees Union v. Logan Valley Plaza*, 391 U.S. 308 (1968). Of these decisions, only the *Lloyd* decision is helpful to Cyber.

In *Greenburgh*, a civic association challenged a federal statue which prohibited the deposit of unstamped "mailable matter" in a letterbox approved by the United States Postal Service. The civic association contended that the First Amendment guaranteed them the right to deposit, without postage, their notices, circulars, flyers in such letterboxes. The Supreme Court upheld the constitutionality of the statute, finding that neither the enactment nor the enforcement of the statute was geared in any way to the content of the message sought to be placed in the letterbox. The Court also noted that the statute did not prevent individuals from going door-to-door to distribute their message or restrict the civic organization's right to use the mails. *Greenburgh*, however, did not involve the issue of whether there was state action. It therefore is inapplicable to the issue of whether AOL's conduct constitutes state action.

In *Logan Valley*, a case involving peaceful picketing directed solely at one establishment within a shopping center, the Court reviewed the *Marsh* decision in detail, emphasized the similarities between a

shopping center and a company town and concluded that a shopping center is the "functional equivalent" of the business district in *Marsh*. As a result, the Court held that the picketers had a First Amendment right to picket within a shopping center. *Logan Valley*, however, was subsequently overruled by *Lloyd,supra*. *Hudgens v. National Labor Relations Board*, 424 U.S. 507 (1976). ("[W]e make clear now, if it was not clear before, that the rationale of *Logan Valley* did not survive the Court's decision in the *Lloyd* case.")

In *Lloyd*, a group of individuals sought to distribute handbills in the interior of a privately owned shopping center. The content of the handbills was not directed at any one establishment in the shopping center but instead was directed at the Vietnam War. The Court noted that, unlike the situation in *Logan Valley* where the protestors had no other alternative to convey their message at the single establishment in the shopping center, the protesters in *Lloyd* could distribute their message about the Vietnam war on any public street, sidewalk or park outside the mall. The Court therefore found that "[i]t would be an unwarranted infringement of property rights to require [the protesters] to yield to the exercise of First Amendment under circumstances where adequate alternative avenues of communication exist." *Lloyd*, 407 U.S. at 567. The *Lloyd* Court went on to reject the individuals' functional equivalency argument, finding that the private shopping center neither assumed the full spectrum of municipal powers nor stood in the shoes of the state, as did the private company in *Marsh*. The Court held that, "[t]he First and Fourteenth Amendments safeguard the rights of free speech and assembly by limitations on *state* action, not on action by the owner of private property used nondiscriminatorily for private purposes only." *Lloyd*, 407 U.S. at 567 (emphasis in original).

Cyber has numerous alternative avenues of sending its advertising to AOL members. An example of another avenue Cyber has of sending its advertising to AOL members over the Internet is the World Wide Web which would allow access by Internet users, including AOL customers, who *want* to receive Cyber's e-mail. Examples of non-Internet avenues include the United States mail, telemarketing, television, cable, newspapers, magazines and even passing out leaflets. Of course, AOL's decision to block Cyber's e-mail from reaching AOL's members does not prevent Cyber from sending its e-mail advertisements to the members of competing commercial online services, including CompuServe, the Microsoft Network and Prodigy.

Having found that AOL is not a state actor under the exclusive public function test, we evaluate whether AOL is a state actor under the remaining two tests, i.e. whether AOL is acting with the help of or in concert with state officials and whether the State has put itself in a position of interdependence with AOL such that it must be considered a participant in AOL's conduct. These tests actually overlap one another.

In its Memorandum, Cyber does not specifically argue that AOL is acting in concert with state officials. Indeed, the two major cases from the Supreme Court which have found state action under this test are clearly distinguishable from the case *sub judice*. *See*, *Adickes v. S.H. Kress & Co.*, 398 U.S. 144 (1970) (finding a conspiracy between a private actor and a state official to engage in unlawful discrimination constituted action under color of law for purposes of 42 U.S.C. Section 1983); *Lugar v. Edmondson Oil Co.*, 457 U.S. 922 (1982) (finding private creditor's pre-judgment attachment petition upon which clerk of state court issued a writ of attachment and sheriff executed the writ on property of private debtor was state action under Section 1983).

Rather, Cyber relies on the "joint participation" doctrine and contends that "AOL's use of the Court to obtain injunctive relief and/or damages [which it seeks in its prayer for relief in its counterclaim] and its assertions of federal and state statutory law, which if applicable to Cyber's activities, would violate Cyber's First Amendment rights." Cyber's Memorandum at 15.

In *Edmonson v. Leesville Concrete Co.*, 500 U.S. 614 (1991) the Supreme Court refined the joint participation test by announcing that courts must ask "first whether the claimed constitutional deprivation resulted from the exercise of a right or privilege having its source in state authority; and second, whether the private party charged with the deprivation could be described in all fairness as a state actor." *Edmonson*, 500 U.S. at 620. Under the first prong, the inquiry is "under what authority did the private person engage in the allegedly unlawful acts." *Mark*, 51 F.3d at 1144.

In the case *sub judice*, the parties have stipulated that "[t]here has been no government involvement in AOL's business decisions with respect to e-mail sent by Cyber nor in any AOL decision to institute or reinstitute a block directed to Internet e-mail sent by Cyber to AOL members or subscribers." Stipulation of Facts at para. 9. As a result, Cyber is unable to satisfy even the first prong of the joint participation test.

In addition, our Court of Appeals has stated that "[m]erely instituting a routine civil suit does not transform a litigant's actions into those taken under color of state law." *Tunstall v. Office of Judicial Support*, 820 F.2d 631, 634 (3d Cir. 1987). The *Tunstall* Court concluded that the filing of a quiet title action in state court by a purchaser of land to complete the seizure of plaintiff's property did not involve state action since the suit "did not attempt any seizure of property with the cooperation of state officials as in the *Lugar* line of cases." *Id.* In addition, the United States Court of Appeals for the Eleventh Circuit has found that a regulated utility did not act under color of state law when it obtained a temporary restraining order from a state court. *Cobb v. Georgia Power Co.*, 757 F.2d 1248 (11th Cir. 1985). The United States Court of Appeals for the Second Circuit has held that the mere filing of a state law contempt proceeding does not constitute joint participation so as to satisfy the color of state law requirement under 42 U.S.C. Section 1983. *Dahlberg v. Becker*, 748 F.2d 85 (2d Cir. 1984).

Perhaps recognizing the futility of its argument, Cyber contends in its Reply Memorandum that "[i]t is not Cyber's position that the mere filing of an action provides a party with the requisite state action to assert a First Amendment violation. Rather it is the Court's participation with the litigant in issuing or enforcing an order which impinges on another's First Amendment rights. *Grandbouche v. Clancey*, 825 F.2d 1463, 1466 (10th Cir. 1987)." Reply Memorandum at 7. In *Grandbouche*, the United States Court of Appeals for the Tenth Circuit stated that the first Amendment "may be applicable in the context of discovery orders, even if all of the litigants are private entities." The Court found government action present as a result of a magistrate's order compelling discovery and the trial court's enforcement of that order.

decision because it has the effect of creating government action every time a magis trate simply signs, and a trial judge enforces, a discovery order. Therefore, even if this Court had enforced a discovery order (which we have not), we would not follow the *Grandbouche* decision.

In sum, we find that since AOL is not a state actor and there has been no state action by AOL's activities under any of the three tests for state action enunciated by our Court of Appeals in *Mark*, Cyber has no right under the First Amendment to the United States Constitution to send unsolicited e-mail to AOL's members. It follows that AOL, as a private company, may block any attempts by Cyber to do so.

Cyber also contends that its practice of sending e-mail advertisements to AOL's servers is also protected "under state constitutional law, which in many instances, affords even broader protection than federal First Amendment guarantees which this Court can enforce." Cyber's Memorandum at 17. Specifically, Cyber refers to the state constitutions of Pennsylvania and Virginia.[3] Although this argument is beyond the scope of the issue the Court directed the parties to brief, we will nevertheless consider it at this time.

The theory that a state constitution's free speech provisions may afford broader rights than similar provisions of the United States Constitution was first recognized by the Supreme Court in *PruneYard Shopping Center v. Robins*, 447 U.S. 74 (1980). The *PruneYard* Court held that, while the First Amendment did not grant the defendants the right to solicit in a privately owned shopping center, state (California) law might grant that right. The Supreme Court of Pennsylvania has itself recognized that "Pennsyl vania may afford greater protection to individual rights under its Constitution" than the Constitution of the United States. *Western Pennsylvania Socialist Workers 1982 Campaign v. Conn.Gen.Life Ins.Co.*, 515 A.2d 1331, 1333-34 (1986) (plurality opinion); *Commonwealth v. Tate*, 432 A.2d 1382 (1981).

Article 1, Section 7 of the Pennsylvania Constitution provides:

> The free communication of thoughts and opin ions is one of the invaluable rights of man,

> and every citizen may freely speak, write and print on any subject ...

In *Tate*, the only case on which Cyber relies, the Supreme Court of Pennsylvania overturned convictions for defiant trespass stemming from a group of protester's refusal to desist from distributing politically oriented materials in a peaceful manner on the campus of a privately owned college. The court found that the college had created a public forum by opening the campus to the public to hear the director of the FBI to speak in a campus building. Because the college had become a public forum and because the defiant trespass statute had provided a defense to a charge of defiant trespass in those circumstances [4], the *Tate* Court held that the protesters had a right to speak freely without fear of criminal conviction under Article I, Section 7 of the Pennsylvania Constitution.

was subsequently clarified by the Supreme Court of Pennsylvania in *Western Pennsylvania Socialist Workers, supra*. In that case, a political committee, its chairman, a gubernatorial candidate and a campaign worker claimed they had the right under, *inter alia*, Article 1, Section 7 of the Pennsylvania Constitution to collect signatures for the gubernatorial candidate's campaign at privately owned shopping malls, including one owned by Connecticut General Life Insurance Co. Connecticut General had a policy which uniformly prohibited all political activities including solicita tion at its mall. The Court distinguished *Tate*, by observing that "[b]y adhering to a strict no political solicitation policy, [Connecticut General] has uniformly and generally prevented the mall from becoming a public forum." *Western Pennsylvania*, 515 A.2d at 1337. Rather, the Court noted that Connecticut General had only invited the public into the mall for commercial purposes. Since Connecticut General had not invited the public into the mall for political purposes, the Court held that Article 1, Section 7, was inapplicable.

The *Western Pennsylvania* Court also rejected attempts to analogize the mall to the company town in *Marsh v. Alabama, supra* by stating:

> A shopping mall is not equivalent to a town. Though it duplicates the commercial function traditionally associated with a town's busi ness district or marketplace, the similarity ends there. People do not live in shopping malls. Malls do not provide essential public services such as water, sewers roads, sanita tion or vital records, nor are they responsi ble for education, recreation or transporta tion. Thus, the *Marsh* analysis is not applicable to the instant case.

The case *sub judice* is more similar to *Western Pennsylva nia* than it is to *Tate*. AOL's e-mail servers are certainly not a traditional public forum such as a street, park or even the college in *Tate*. Instead, AOL's e-mail servers are privately owned and are only available to the subscribers of AOL who pay a fee for their usage. Moreover, unlike *Tate*, AOL has not presented its e-mail servers to the public at large for disseminating political messages at a certain event. Indeed, AOL has never presented its e-mail servers to the public at large for dissemination of messages in general as AOL's servers have a finite capacity. Stipulation of Facts at para. 7. As noted above, AOL's e-mail system simply provides a means for its members to communicate with those members of the public who are connected with the Internet.

Cyber also does not have the right under the Constitution of Virginia to send unsolicited e-mail over the Internet to AOL members.Article I, Section 12 of the Virginia Constitution provides:

> That the freedoms of speech and of the press are among the great bulwarks of liberty, and can never be restrained except by despotic governments; that any citizen may freely speak, write, and publish his sentiments on all subjects, being responsible for the abuse of that right; that the General Assembly shall not pass any law abridging the freedom of speech or of the press, nor the right of the people peaceably to assemble, and to petition the government for the redress of grievances.

There are no decisions which interpret this provision in a manner which would be helpful to Cyber. The decisions Cyber cites, *National Capital Naturists, Inc. v. Board of Supervisors*, 878 F.2d 128, 133 (4th Cir. 1989); *Leachman v. Rector & Visitors of the Univ. of Virginia*, 691 F.Supp. 961, 964 n.5 (W.D.Va. 1988), *aff'd*, 915 F.2d 1564 (4th Cir. 1990); *Robert v. Norfolk*, 188 Va. 413, 49 S.E.2d 697, 700 (1948) all merely recognize the principle enunciat ed by the Supreme Court in *PruneYard* that states have the

"sovereign right" to give their constitutions an expansive interpreta tion.

Although we have found that Cyber has no right under the First Amendment of the United States Constitution or under the Constitutions of Pennsylvania or Virginia to send unsolicited e-mail to members of AOL, we will not, at this time, enter judgment on Count V of Cyber's First Amended Complaint for declaratory relief. This is because Cyber contends in its Reply brief that "many more issues ... have to be addressed since there are numerous reasons beyond the First Amendment which will permit Cyber to send e-mail to AOL members." Cyber's Reply Memorandum at 1. Therefore, we will simply declare that Cyber has no right under the First Amendment to the United States Constitution or under the Constitu tions of Pennsylvania or Virginia to send unsolicited e-mail over the Internet to members of AOL. We will allow Cyber ten days from the date of this Memorandum Opinion and Order to submit a list of the theories other than the First Amendment it believes entitles it to send unsolicited e-mail to members of AOL.

An Order to that effect follows.

FOOTNOTES

1. In past submissions, Cyber has stated that AOL's "e-mail bombs" occurred when AOL gathered all unsolicited e-mail sent by Cyber to undeliverable AOL addresses, altered the return path of such e-mail, and then sent the altered e-mail in a bulk transmis sion to Cyber's ISPs in order to disable the ISPs.

2. Indeed, our Court of Appeals has observed that the exclusive public function test itself "rarely could be satisfied." *Mark*, 51 F.3d at 1142. "Thus, in *Jackson v. Metropolitan Edison Co.*, 419 U.S. 345 (1974), the Court held that a private utility company, extensively regulated by the state, and apparently holding at least a partial monopoly in its territory, did not act under color of state law, in part because the state where the utility was engaged in business had `rejected the contention that the furnishing of utility services is either a state function or a municipal duty.' (citation omitted). Similarly, in *Rendell-Baker v. Kohn*, 457 U.S. 830 (1982), the Court held that a private entity engaged in the education of maladjusted high school students did not perform an exclusively public function because `[the state's] legislative policy choice [to fund the public school] in no way makes these services the exclusive province of the State.' (citation omitted); *see also Black v. Indiana Area Sch. Dist.*, 985 F.2d 707, 710-11 (3d Cir. 1993) (private contractor providing state school bus program at state expense not performing exclusive state function)." *Mark, id.*

3. Cyber contends it is entitled to the protection of the Pennsylvania Constitution because Cyber's e-mail originates from Pennsylvania and that it is entitled to the protection of the Virginia Constitution because AOL's blocking actions occur in Virginia.

4. Pa.Cons.Stat.Ann. tit. 18 Section 3503(c)(2) provides:

> It is a defense to prosecution under this section that: the premises were at the time open to members of the public and the actor complied with all lawful conditions imposed on access to or remaining on the premises.

© 1997 The Bureau of National Affairs Inc., All Rights Reserved

BNA | TOP STORY | LIBRARY | FEEDBACK | SALES INFO

THE BUREAU OF NATIONAL AFFAIRS INC.

ELECTRONIC COMMERCE & LAW REPORT

MARKING 50 YEARS OF EMPLOYEE OWNERSHIP

Updated: 12/01/97 10:48 AM Eastern Standard Time

IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF PENNSYLVANIA

ZIPPO MANUFACTURING COMPANY Plaintiff
v.
ZIPPO DOT COM, INC. Defendant.

Civil Action No. 96-397 Erie

January 16, 1997

MEMORANDUM OPINION

McLAUGHLIN, J.

This is an Internet domain name [1] dispute. At this stage of the controversy, we must decide the Constitutionally permissible reach of Pennsylvania's Long Arm Statute, 42 Pa.C.S.A. §5322, through cyberspace. Plaintiff Zippo Manufacturing Corporation ("Manufacturing") has filed a five count complaint against Zippo Dot Com, Inc. ("Dot Com") alleging trademark dilution, infringement, and false designation under the Federal Trademark Act, 15 U.S.C. §§1051-1127. In addition, the Complaint alleges causes of action based on state law trademark dilution under 54 Pa.C.S.A. §1124, and seeks equitable accounting and imposition of a constructive trust. Dot Com has moved to dismiss for lack of personal jurisdiction and improper venue pursuant to Fed.R.Civ.P. 12(b)(2) and (3) or, in the alternative, to transfer the case pursuant to 28 U.S.C. §1406(a). For the reasons set forth below, Defendant's motion is denied.

I. BACKGROUND

The facts relevant to this motion are as follows. Manufacturing is a Pennsylvania corporation with its principal place of business in Bradford, Pennsylvania. Manufacturing makes, among other things, well known "Zippo" tobacco lighters. Dot Com is a California corporation with its principal place of business in Sunnyvale, California. Dot Com operates an Internet Web Site [2] and an Internet news service and has obtained the exclusive right to use the domain names "zippo.com", "zippo.net" and "zipponews.com" on the Internet. [3]

Dot Com's Web site contains information about the company, advertisements and an application for its Internet news service. The news service itself consists of three levels of membership -- public/free, "Original" and "Super." Each successive level offers access to a greater number of Internet newsgroups. A customer who wants to subscribe to either the "Original" or "Super" level of service fills out an on-line application that asks for a variety of information including the person's name and address. Payment is made by credit card over the Internet or the telephone. The application is then processed and the subscriber is assigned a password which permits the subscriber to view and/or download Internet newsgroup messages that are stored on the Defendant's server in California.

Dot Com's contacts with Pennsylvania have occurred almost exclusively over the Internet. Dot Com's offices, employees and Internet servers are located in California. Dot Com maintains no offices, employees or agents in Pennsylvania. Dot Com's advertising for its service to Pennsylvania residents involves posting information about its service on its Web page, which is accessible to Pennsylvania residents via the Internet. Defendant has approximately 140,000 paying subscribers worldwide. Approximately two percent (3,000) of those subscribers are Pennsylvania residents. These subscribers have contracted to receive Dot Com's service by visiting its Web site and filling out the application. Additionally, Dot Com has entered into agreements with seven Internet access providers in Pennsylvania to permit their subscribers to access Dot Com's news service. Two of these providers are located in the Western District of Pennsylvania.

The basis of the trademark claims is Dot Com's use of the word "Zippo" in the domain names it holds, in numerous locations in its Web site and in the heading of Internet newsgroup messages that have been posted by Dot Com subscribers. When an Internet user views or downloads a newsgroup message posted by a Dot Com subscriber, the word "Zippo" appears in the "Message-Id" and "Organization" sections of the heading. [4] The news message itself, containing text and/or pictures, follows. Manufacturing points out that some of the messages contain adult oriented, sexually explicit subject matter.

II. STANDARD OF REVIEW

When a defendant raises the defense of the court's lack of personal jurisdiction, the burden falls upon the plaintiff to come forward with sufficient facts to establish that jurisdiction is proper. **Mellon Bank (East) PSFS, N.A. v. Farino,** 960 F.2d 1217, 1223 (3d Cir. 1992) (**citing Carteret Savings Bank v. Shusan**, 954 F.2d 141 (3d Cir. 1992), **cert. denied** 506 U.S. 817 (1992)). The plaintiff meets this burden by making a prima facie showing of "sufficient contacts between the defendant and the forum state." **Mellon East,** 960 F.2d at 1223 (**citing Provident Nat. Bank v. California Fed. Sav. & Loan Assoc.,** 819 F.2d 434 (3d Cir. 1987)).

III. DISCUSSION

A. Personal Jurisdiction

1. The Traditional Framework

Our authority to exercise personal jurisdiction in this case is conferred by state law. Fed.R.Civ.P. 4(e); **Mellon**, 960 F.2d at 1221. The extent to which we may exercise that authority is governed by the Due Process Clause of the Fourteenth Amendment to the Federal Constitution. **Kulko v. California Supreme Court**, 436 U.S. 84, 91 (1978).

Pennsylvania's long arm jurisdiction statute is codified at 42 Pa.C.S.A. §5322(a). The portion of the statute authorizing us to exercise jurisdiction here permits the exercise of jurisdiction over non-resident defendants upon:

(2) Contracting to supply services or things in this Commonwealth.

42 Pa.C.S.A. §5322(a). It is undisputed that Dot Com contracted to supply Internet news services to approximately 3,000 Pennsylvania residents and also entered into agreements with seven Internet access providers in Pennsylvania. Moreover, even if Dot Com's conduct did not satisfy a specific provision of the statute, we would nevertheless be authorized to exercise jurisdiction to the "fullest extent allowed under the Constitution of the United States." 42 Pa.C.S.A. §5322(b).

The Constitutional limitations on the exercise of personal jurisdiction differ depending upon whether a court seeks to exercise general or specific jurisdiction over a non-resident defendant. **Mellon,** 960 F.2d at 1221. General jurisdiction permits a court to exercise personal jurisdiction over a non-resident defendant for non-forum related activities when the defendant has engaged in "systematic and

continuous" activities in the forum state. **Helicopteros Nacionales de Columbia , S.A. v. Hall,** 466 U.S. 408, 414-16 (1984). In the absence of general jurisdiction, specific jurisdiction permits a court to exercise personal jurisdiction over a non-resident defendant for forum-related activities where the "relationship between the defendant and the forum falls within the `minimum contacts' framework" of **International Shoe Co. v. Washington,** 326 U.S. 310 (1945) and its progeny. **Mellon,** 960 F.2d at 1221. Manufacturing does not contend that we should exercise general personal jurisdiction over Dot Com. Manufacturing concedes that if personal jurisdiction exists in this case, it must be specific.

A three-pronged test has emerged for determining whether the exercise of specific personal jurisdiction over a non-resident defendant is appropriate: (1) the defendant must have sufficient "minimum contacts" with the forum state, (2) the claim asserted against the defendant must arise out of those contacts, and (3) the exercise of jurisdiction must be reasonable. **Id.** The "Constitutional touchstone" of the minimum contacts analysis is embodied in the first prong, "whether the defendant purposefully established" contacts with the forum state. **Burger King Corp. v. Rudzewicz,** 471 U.S. 462, 475 (1985) (**citing International Shoe Co. v. Washington,** 326 U.S. 310, 319 (1945)). Defendants who "`reach out beyond one state' and create continuing relationships and obligations with the citizens of another state are subject to regulation and sanctions in the other State for consequences of their actions." **Id. (citing Travelers Health Assn. v. Virginia,** 339 U.S. 643, 647 (1950)). "[T]he foreseeability that is critical to the due process analysis is ... that the defendant's conduct and connection with the forum State are such that he should reasonably expect to be haled into court there." **World Wide Volkswagen Corp. v. Woodson,** 444 U.S. 286, 295 (1980). This protects defendants from being forced to answer for their actions in a foreign jurisdiction based on "random, fortuitous or attenuated" contacts. **Keeton v. Hustler Magazine, Inc.,** 465 U.S. 770, 774 (1984). "Jurisdiction is proper, however, where contacts proximately result from actions by the defendant **himself** that create a `substantial connection' with the forum State." **Burger King,** 471 U.S. at 475 (**citing McGee v. International Life Insurance Co.,** 355 U.S. 220, 223 (1957)).

The "reasonableness" prong exists to protect defendants against unfairly inconvenient litigation. **World Wide Volkswagen,** 444 U.S. at 292. Under this prong, the exercise of jurisdiction will be reasonable if it does not offend "traditional notions of fair play and substantial justice." **International Shoe,** 326 U.S. at 316. When determining the reasonableness of a particular forum, the court must consider the burden on the defendant in light of other factors including: "the forum state's interest in adjudicating the dispute; the plaintiff's interest in obtaining convenient and effective relief, at least when that interest is not adequately protected by the plaintiff's right to choose the forum; the interstate judicial system's interest in obtaining the most efficient resolution of controversies; and the shared interest of the several states in furthering fundamental substantive social policies." **World Wide Volkswagen,** 444 U.S. at 292 (internal citations omitted).

2. The Internet and Jurisdiction

In **Hanson v. Denckla,** the Supreme Court noted that "[a]s technological progress has increased the flow of commerce between States, the need for jurisdiction has undergone a similar increase." **Hanson v. Denckla,** 357 U.S. 235, 250-51 (1958). Twenty seven years later, the Court observed that jurisdiction could not be avoided "merely because the defendant did not **physically** enter the forum state. **Burger King,** 471 U.S. at 476.

The Court observed that:

[I]t is an inescapable fact of modern commercial life that a substantial amount of commercial business is transacted solely by mail and wire communications across state lines, thus obviating the need for physical presence within a State in which business is conducted.

Id.

Enter the Internet, a global "`super-network' of over 15,000 computer networks used by over 30 million individuals, corporations, organizations, and educational institutions worldwide." **Panavision Intern., L.P. v. Toeppen,** 938 F.Supp. 616 (S.D.Cal. 1996) (**citing American Civil Liberties Union v. Reno,**

929 F.Supp. 824, 830-48 (E.D.Pa. 1996). "In recent years, businesses have begun to use the Internet to provide information and products to consumers and other businesses." **Id.** The Internet makes it possible to conduct business throughout the world entirely from a desktop. With this global revolution looming on the horizon, the development of the law concerning the permissible scope of personal jurisdiction based on Internet use is in its infant stages. The cases are scant. Nevertheless, our review of the available cases and materials [5] reveals that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction if proper. **E.g. Compuserve, Inc. v. Patterson,** 89 F.2d 1257 (6th Cir. 1996). At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction. **E.g. Bensusan Restaurant Corp., v. King,** 937 F.Supp. 296 (S.N.D.Y. 1996). The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site. **E.g. Maritz, Inc. v. Cybergold, Inc.,** 1996 U.S. Dist. Lexis 14976 (E.D.Mo. Aug. 19, 1996).

Traditionally, when an entity intentionally reaches beyond its boundaries to conduct business with foreign residents, the exercise of specific jurisdiction is proper. **Burger King,** 471 U.S. at 475. Different results should not be reached simply because business is conducted over the Internet. In **Compuserve, Inc. v. Patterson,** 89 F.2d 1257 (6th Cir. 1996), the Sixth Circuit addressed the significance of doing business over the Internet. In that case, Patterson, a Texas resident, entered into a contract to distribute shareware [6] through Compuserve's Internet server located in Ohio. **Compuserve,** 89 F.2d at 1260. From Texas, Patterson electronically uploaded thirty-two master software files to Compuserve's server in Ohio via the Internet. **Id.** at 1261. One of Patterson's software products was designed to help people navigate the Internet. **Id.** When Compuserve later began to market a product that Patterson believed to be similar to his own, he threatened to sue. **Id.** Compuserve brought an action in the Southern District of Ohio, seeking a declaratory judgment. **Id.** The District Court granted Patterson's motion to dismiss for lack of personal jurisdiction and Compuserve appealed. **Id.** The Sixth Circuit reversed, reasoning that Patterson had purposefully directed his business activities toward Ohio by knowingly entering into a contract with an Ohio resident and then "deliberately and repeatedly" transmitted files to Ohio. **Id.** at 1264-66.

In **Maritz, Inc. v. Cybergold, Inc.,** 1996 U.S. Dist. Lexis 14976 (E.D.Mo. Aug. 19, 1996), the defendant had put up a Web site as a promotion for its upcoming Internet service. The service consisted of assigning users an electronic mailbox and then forwarding advertisements for products and services that matched the users' interests to those electronic mailboxes. **Maritz,** 1996 U.S. Dist. Lexis 14976 at *7. The defendant planned to charge advertisers and provide users with incentives to view the advertisements. **Id.** Although the service was not yet operational, users were encouraged to add their address to a mailing list to receive updates about the service. **Id.** The court rejected the defendant's contention that it operated a "passive Web site." **Id.** at * 16. The court reasoned that the defendant's conduct amounted to "active solicitations" and "promotional activities" designed to "develop a mailing list of Internet users" and that the defendant "indiscriminately responded to every user" who accessed the site. **Id.** at *14-17.

Inset Systems, Inc. v. Instruction Set, 937 F.Supp. 161 (D. Conn. 1996) represents the outer limits of the exercise of personal jurisdiction based on the Internet. In **Inset Systems,** a Connecticut corporation sued a Massachusetts corporation in the District of Connecticut for trademark infringement based on the use of an Internet domain name. **Inset Systems,** 937 F.Supp. at 162. The defendant's contacts with Connecticut consisted of posting a Web site that was accessible to approximately 10,000 Connecticut residents and maintaining a toll free number. **Id.** at 165. The court exercised personal jurisdiction, reasoning that advertising on the Internet constituted the purposeful doing of business in Connecticut because "unlike television and radio advertising, the advertisement is available continuously to any

Internet user." **Id.** at 165.

Bensusan Restaurant Corp., v. King, 937 F.Supp. 296 (S.D. N.Y. 1996) reached a different conclusion based on a similar Web site. In **Bensusan,** the operator of a New York jazz club sued the operator of a Missouri jazz club for trademark infringement. Bensusan, 937 F.Supp. at 297. The Internet Web site at issue contained general information about the defendant's club, a calendar of events and ticket information. **Id.** However, the site was not interactive. **Id.** If a user wanted to go to the club, she would have to call or visit a ticket outlet and then pick up tickets at the club on the night of the show. **Id.** The court refused to exercise jurisdiction based on the Web site alone, reasoning that it did not rise to the level of purposeful availment of that jurisdiction's laws. The court distinguished the case from Compuserve, **supra**, where the user had "`reached out' from Texas to Ohio and `originated and maintained' contacts with Ohio." **Id.** at 301.

Pres-Kap, Inc. v. System One Direct Access, Inc., 636 So.2d 1351 (Fla. App. 1994), **review denied** , 645 So.2d 455 (Fla. 1994) is not inconsistent with the above cases. In **Pres-Kap**, a majority of a three-judge intermediate state appeals court refused to exercise jurisdiction over a consumer of an on-line airline ticketing service. **Pres-Kap** involved a suit on a contract dispute in a Florida court by a Delaware corporation against its New York customer. **Pres-Kap**, 636 So.2d at 1351-52. The defendant had leased computer equipment which it used to access an airline ticketing computer located in Florida. **Id.** The contract was solicited, negotiated, executed and serviced in New York. **Id.** at 1252. The defendant's only contact with Florida consisted of logging onto the computer located in Florida and mailing payments for the leased equipment to Florida. **Id.** at 1253. **Pres-Kap** is distinguishable from the above cases and the case at bar because it addressed the exercise of jurisdiction over a consumer of on-line services as opposed to a provider. When a consumer logs onto a server in a foreign jurisdiction he is engaging in a fundamentally different type of contact than an entity that is using the Internet to sell or market products or services to residents of foreign jurisdictions. The **Pres-Kap** court specifically expressed concern over the implications of subjecting users of "on-line" services with contracts with out-of-state networks to suit in foreign jurisdictions. **Id.** at 1353.

3. Application to this Case

First, we note that this is not an Internet advertising case in the line of **Inset Systems** and **Bensusan, supra**. Dot Com has not just posted information on a Web site that is accessible to Pennsylvania residents who are connected to the Internet. This is not even an interactivity case in the line of **Maritz** , **supra**. Dot Com has done more than create an interactive Web site through which it exchanges information with Pennsylvania residents in hopes of using that information for commercial gain later. We are not being asked to determine whether Dot Com's Web site alone constitutes the purposeful availment of doing business in Pennsylvania. This is a "doing business over the Internet" case in the line of **Compuserve, supra.** We are being asked to determine whether Dot Com's conducting of electronic commerce with Pennsylvania residents constitutes the purposeful availment of doing business in Pennsylvania. We conclude that it does. Dot Com has contracted with approximately 3,000 individuals and seven Internet access providers in Pennsylvania. The intended object of these transactions has been the downloading of the electronic messages that form the basis of this suit in Pennsylvania.

We find Dot Com's efforts to characterize its conduct as falling short of purposeful availment of doing business in Pennsylvania wholly unpersuasive. At oral argument, Defendant repeatedly characterized its actions as merely "operating a Web site" or "advertising." Dot Com also cites to a number of cases from this Circuit which, it claims, stand for the proposition that merely advertising in a forum, without more, is not a sufficient minimal contact. [7] This argument is misplaced. Dot Com has done more than advertise on the Internet in Pennsylvania. Defendant has sold passwords to approximately 3,000 Subscribers in Pennsylvania and entered into seven contracts with Internet access providers to furnish its services to their customers in Pennsylvania.

Dot Com also contends that its contacts with Pennsylvania residents are "fortuitous" within the meaning of **World Wide Volkswagen**, 444 U.S. 286 (1980). Defendant argues that it has not "actively" solicited business in Pennsylvania and that any business it conducts with Pennsylvania residents has resulted from contacts that were initiated by Pennsylvanians who visited the Defendant's Web site. The fact that Dot

Com's services have been consumed in Pennsylvania is not "fortuitous" within the meaning of **World Wide Volkswagen**. In **World Wide Volkswagen**, a couple that had purchased a vehicle in New York, while they were New York residents, were injured while driving that vehicle through Oklahoma and brought suit in an Oklahoma state court. **World Wide Volkswagen**, 444 U.S. at 288. The manufacturer did not sell its vehicles in Oklahoma and had not made an effort to establish business relationships in Oklahoma. **Id.** at 295. The Supreme Court characterized the manufacturer's ties with Oklahoma as fortuitous because they resulted entirely out the fact that the plaintiffs had driven their car into that state. **Id.**

Here, Dot Com argues that its contacts with Pennsylvania residents are fortuitous because Pennsylvanians happened to find its Web site or heard about its news service elsewhere and decided to subscribe. This argument misconstrues the concept of fortuitous contacts embodied in **World Wide Volkswagen**. Dot Com's contacts with Pennsylvania would be fortuitous within the meaning of **World Wide Volkswagen** if it had no Pennsylvania subscribers and an Ohio subscriber forwarded a copy of a file he obtained from Dot Com to a friend in Pennsylvania or an Ohio subscriber brought his computer along on a trip to Pennsylvania and used it to access Dot Com's service. That is not the situation here. Dot Com repeatedly and consciously chose to process Pennsylvania residents' applications and to assign them passwords. Dot Com knew that the result of these contracts would be the transmission of electronic messages into Pennsylvania. The transmission of these files was entirely within its control. Dot Com cannot maintain that these contracts are "fortuitous" or "coincidental" within the meaning of **World Wide Volkswagen**. When a defendant makes a conscious choice to conduct business with the residents of a forum state, "it has clear notice that it is subject to suit there." **World Wide Volkswagen**, 444 U.S. at 297. Dot Com was under no obligation to sell its services to Pennsylvania residents. It freely chose to do so, presumably in order to profit from those transactions. If a corporation determines that the risk of being subject to personal jurisdiction in a particular forum is too great, it can choose to sever its connection to the state. **Id.** If Dot Com had not wanted to be amenable to jurisdiction in Pennsylvania, the solution would have been simple -- it could have chosen not to sell its services to Pennsylvania residents.

Next, Dot Com argues that its forum-related activities are not numerous or significant enough to create a "substantial connection" with Pennsylvania. Defendant points to the fact that only two percent of its subscribers are Pennsylvania residents. However, the Supreme Court has made clear that even a single contact can be sufficient. **McGee**, 355 U.S. at 223. The test has always focused on the "nature and quality" of the contacts with the forum and not the quantity of those contacts. **International Shoe**, 326 U.S. at 320. The Sixth Circuit also rejected a similar argument in **Compuserve** when it wrote that the contacts were "deliberate and repeated even if they yielded little revenue." **Compuserve**, 89 F.2d at 1265.

We also conclude that the cause of action arises out of Dot Com's forum-related conduct in this case. The Third Circuit has stated that "a cause of action for trademark infringement occurs where the passing off occurs." **Cottman Transmission Systems Inc. v. Martino,** 36 F.3d 291, 294 **(citing Tefal, S.A. v. Products Int'l Co.,** 529 F.2d 495, 496 n.1 (3d Cir. 1976); **Indianapolis Colts v. Metro. Baltimore Football**, 34 F.3d 410 (7th Cir. 1994). In **Tefal**, the maker and distributor of T-Fal cookware sued a partnership of California corporations in the District of New Jersey for trademark infringement. **Tefal**, 529 F.2d at 496. The defendants objected to venue in New Jersey, arguing that the contested trademark accounted for only about five percent of national sales. **Id.** On appeal, the Third Circuit concluded that since substantial sales of the product bearing the allegedly infringing mark took place in New Jersey, the cause of action arose in New Jersey and venue was proper. **Tefal**, 529 F.2d at 496-97.

In **Indianapolis Colts,** also case cited by the Third Circuit in **Cottman**, an Indiana National Football League franchise sued a Maryland Canadian Football League franchise in the Southern District of Indiana, alleging trademark infringement. **Indianapolis Colts**, 34 F.3d at 411. On appeal, the Seventh Circuit held that personal jurisdiction was appropriate in Indiana because trademark infringement is a tort-like injury and a substantial amount of the injury from the alleged infringement was likely to occur in Indiana. **Id.** at 412.

In the instant case, both a significant amount of the alleged infringement and dilution, and resulting

injury have occurred in Pennsylvania. The object of Dot Com's contracts with Pennsylvania residents is the transmission of the messages that Plaintiff claims dilute and infringe upon its trademark. When these messages are transmitted into Pennsylvania and viewed by Pennsylvania residents on their computers, there can be no question that the alleged infringement and dilution occur in Pennsylvania. Moreover, since Manufacturing is a Pennsylvania corporation, a substantial amount of the injury from the alleged wrongdoing is likely to occur in Pennsylvania. Thus, we conclude that the cause of action arises out of Dot Com's forum-related activities under the authority of both **Tefal and Indianapolis Colts, supra.**

Finally, Dot Com argues that the exercise of jurisdiction would be unreasonable in this case. We disagree. There can be no question that Pennsylvania has a strong interest in adjudicating disputes involving the alleged infringement of trademarks owned by resident corporations. We must also give due regard to the Plaintiff's choice to seek relief in Pennsylvania. **Kulko,** 436 U.S. at 92. These concerns outweigh the burden created by forcing the Defendant to defend the suit in Pennsylvania, especially when Dot Com consciously chose to conduct business in Pennsylvania, pursuing profits from the actions that are now in question. The Due Process Clause is not a "territorial shield to interstate obligations that have been voluntarily assumed." **Burger King,** 471 U.S. at 474.

B. Venue Under 28 U.S.C. §1391

Defendant argues that, under the law of this Circuit, venue is only proper in trademark cases in the judicial district in which "a substantial part of the events or omissions giving rise to the claim occurred." In support of this proposition, Defendant cites **Cottman Transmission Systems, Inc. v. Martino,** 36 F.3d 291 (3d Cir. 1994). We cannot agree.

Venue in this case is governed by 28 U.S.C. §1391(b), the relevant portion of which provides:

(b) A civil action wherein jurisdiction is not founded solely on diversity of citizenship may, except as otherwise provided by law, be brought only in (1) a judicial district where any defendant resides, if all defendants reside in the same State, (2) a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred, or a substantial part of the property that is the subject of the action is situated, or (3) a judicial district in which the defendant may be found if there is no district in which the action may otherwise be brought.

28 U.S.C. §1391(b). Subsection (c) further provides that a corporate defendant is "deemed to reside in any judicial district in which it is subject to personal jurisdiction at the time the action is commenced." 28 U.S.C. §1391(c). Dot Com is the only defendant in this case and it is a corporation. Thus, under the plain language of 28 U.S.C. §1391(b)(1), our previous discussion of personal jurisdiction is dispositive of the venue issue. Contrary to Dot Com's contention, **Cottman** does not command a different result.

Cottman involved a suit by a Pennsylvania corporation against a former Michigan franchisee and his wholly owned corporation for trademark infringement arising out of the continued use of the plaintiff's trademark after termination of the franchise agreement. The suit was brought in the Eastern District of Pennsylvania. Both defendants were Michigan residents and the corporation did business exclusively in Michigan. In the district court, the plaintiff relied exclusively on 28 U.S.C. §1391(b)(2) to establish venue. The district court found venue proper, reasoning that a "substantial part of the events or omissions giving rise to the claim occurred" in Pennsylvania. **Cottman Transmission v. Metro Distributing,** 796 F.Supp. 838, 844 (E.D. Pa. 1992). Thus, on appeal, the only issue before the Third Circuit was the propriety of venue under §1391(b)(2). In fact, the Third Circuit expressly stated that it was analyzing the case under §1391(b)(2). **Cottman,** 36 F.3d at 294. The Third Circuit read the record as only capable of supporting the contention that the defendants attempted to pass off the trademarks at issue in the Eastern District of Michigan. **Id.** at 296. Thus, the Third Circuit reversed, because a "substantial part of the events or omissions giving rise to the claim" had not occurred in the Eastern District of Pennsylvania. **Id.**

The fact that the Third Circuit analyzed **Cottman** under the standard in §1391(b)(2) does not mean that it applies to every trademark case. In fact, at oral argument, Dot Com conceded that if its reading of **Cottman** were the law, it would effectively render §1391(b)(1) inapplicable to trademark cases and

require the plaintiff to always satisfy §1391(b)(2) in order to lay venue. If the Third Circuit had intended to create such a radical departure from the plain language of §1391, it would have said so.

Since venue has been properly laid in this District, we cannot dismiss the action under 28 U.S.C. §1406(a). **Jumara v. State Farm Inc. Co.,** 55 F.3d 873, 877 (3d Cir. 1995). We are also not permitted to compel the Plaintiff to accept a transfer against its wishes. **Carteret v. Shusan,** 919 F.2d 225, 232 (3d Cir. 1990).

IV. CONCLUSION

We conclude that this Court may appropriately exercise personal jurisdiction over the Defendant and that venue is proper in this judicial district. An appropriate order follows.

ORDER

McLAUGHLIN, J.

AND NOW, this 16th day of January 1997, IT IS HEREBY ORDERED that Defendant Zippo Dot Com's Motion to Dismiss for Improper Venue and Transfer under 28 U.S.C. §1406(a); Alternatively to Dismiss for Lack of Personal Jurisdiction [Doc. No. 9] is DENIED.

Sean J. McLaughlin

United States District Judge

cm: All parties of record.

End Notes

1. Return to Text Domain names serve as a primary identifier of an Internet user. **Panavision Intern., L.P. v. Toeppen,** 938 F.Supp. 616 (S.D. Cal. 1996). Businesses using the Internet commonly use their business names as part of the domain name (e.g. IBM.com). **Id.** The designation ".com" identifies the user as a commercial entity. **Id.**

2. Return to Text A "site" is an Internet address that permits the exchange of information with a host computer. **Bensusan Restaurant Corp. v. King,** 937 F.Supp. 295 (S.D.N.Y. 1996). The "Web" or "World Wide Web" refers to the collection of sites available on the Internet. **Id.**

3. Return to Text Dot Com has registered these domain names with Network Solutions, Inc. which has contracted with the National Science Foundation to provide registration services for Internet domain names. Once a domain name is registered to one user, it may not be used by another.

4. Return to Text For example, a typical message heading might appear as:

Subject: subject of the message From: name of person posting message Date: date posted Message-Id: identifying#ews.zippo.com Reference: reference# Organization: Zippo Newsgroups: news groups to which sender has subscribed The italicized text represents a generic description of specific information appearing in the message.

5. Return to Text **See, generally,** Robert A. Bourque and Kerry L. Konrad, **Avoiding Jurisdiction Based on Internet Web Site,** New York Law Journal (Dec. 10, 1996); David Bender, **Emerging Personal Jurisdiction Issues on the Internet,** 453 PLI/Pat 7 (1996); Comment, Richard S. Zembek, **Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace,** 6 Alb. L.J. Sci. & Tech. 339 (1996).

6. Return to Text "Shareware" is software which a user is permitted to download and use for a trial

period, after which the user is asked to pay a fee to the author for continued use. **Compuserve,** 89 F.2d at 1260. 7 Defendant has cited to: **Gehling v. St. George's School of Medicine, Ltd.,** 773 F.2d 539 (1985); **Fields v. Ramada Inn Inc.,** 816 F.Supp. 1033 (E.D. Pa. 1993); and **Garofalo v. Praiss,** 1990 WL 97800 (E.D.Pa. 1990). We note that these cases all involve the issue of whether advertising can rise to the level of "systematic and continuous" contacts for the purpose of general jurisdiction.

© 1997 The Bureau of National Affairs, Inc., All Rights Reserved

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN LIBRARY ASSOCIATION; FREEDOM TO READ FOUNDATION, INC.; NEW YORK LIBRARY ASSOCIATION; WESTCHESTER LIBRARY SYSTEM; AMERICAN BOOKSELLERS FOUNDATION FOR FREE EXPRESSION; ASSOCIATION OF AMERICAN PUBLISHERS, INC.; BIBLIOBYTES, INC.; MAGAZINE PUBLISHERS OF AMERICA, INC.; INTERACTIVE DIGITAL SOFTWARE ASSOCIATION; PUBLIC ACCESS NETWORKS CORPORATION; ECHO; NEW YORK CITY NET; ART ON THE NET; PEACEFIRE; and AMERICAN CIVIL LIBERTIES UNION,
Plaintiffs,

-against

GEORGE PATAKI, in his official capacity as Governor of the State of New York; and DENNIS VACCO, in his official capacity as Attorney General of the State of New York,
Defendants.

97 Civ. 0222 (LAP)

OPINION

LORETTA A. PRESKA, United States District Judge:

The Internet may well be the premier technological innovation of the present age. Judges and legislators faced with adapting existing legal standards to the novel environment of cyberspace struggle with terms and concepts that the average American five-year-old tosses about with breezy familiarity.[1] Not surprisingly, much of the legal analysis of Internet-related issues has focused on seeking a familiar analogy for the unfamiliar. Commentators reporting on the recent oral argument before the Supreme Court of the United States, which is considering a First Amendment challenge to the Communications Decency Act, noted that the Justices seemed bent on finding the appropriate analogy which would tie the Internet to some existing line of First Amendment jurisprudence: is the Internet more like a television? a radio? a newspaper? a 900-line? a village green? See. e.g., Linda Greenhouse, What Level of Protection for Internet Speech? High Court Weighs Decency-Act Case, N. Y. Times, March 24, 1997, at C5; see also Denver Area Educ. Telecommunications Consortium v. Federal Communics. Comm'n, 116 S. Ct. 2374, 2419-21 (1996) (Thomas, J., concurring in the judgment and dissenting in part) (criticizing the majority for declining to determine whether cable television is more closely analogous, for purposes of First Amendment analysis, to a print medium or a broadcast medium). This case, too, depends on the appropriate analogy. I find, as described more fully below, that the

case, too, depends on the appropriate analogy. I find, as described more fully below, that the Internet is analogous to a highway or railroad. This determination means that the phrase "information superhighway" is more than a mere buzzword; it has legal significance, because the similarity between the Internet and more traditional instruments of interstate commerce leads to analysis under the Commerce Clause.

BACKGROUND

The plaintiffs in the present case filed this action challenging New York Penal Law § 235.21(3) (the "Act" or the "New York Act"), seeking declaratory and injunctive relief. Plaintiffs contend that the Act is unconstitutional both because it unduly burdens free speech in violation of the First Amendment and because it unduly burdens interstate commerce in violation of the Commerce Clause. Plaintiffs moved for a preliminary injunction enjoining enforcement of the Act; defendants opposed the motion. A factual hearing was held from April 3 to April 7, 1997 and oral argument conducted on April 22, 1997. For the reasons that follow, the motion for a preliminary injunction is granted.

I. Parties to the Action

Plaintiffs in the present action represent a spectrum of individuals and organizations who use the Internet to communicate, disseminate, display, and access a broad range of communications. All of the plaintiffs communicate online both within and outside the State of New York, and each plaintiff's communications are accessible from within and outside New York. Plaintiffs include:

· American Library Association, Freedom to Read Foundation, Inc., New York Library Association, and Westchester Library System are organizations representing the interests of libraries. Libraries serve as both access and content providers on the Internet, providing their patrons with facilities to access the Internet. Libraries also post their card catalogues, information about upcoming events and online versions of text or art from their collections, as well as sponsoring chat rooms.

· American Booksellers Foundation For Free Expression ("ABFFE") is a national association of general interest and specialized bookstores formed to protect free expression rights. ABFFE has many members who use the Internet and electronic communications to obtain from publishers information and excerpts, some of which may contain sexually explicit passages.

· Association of American Publishers ("AAP") is a national association of publishers of general books, textbooks, and educational materials. AAP has many members who actively use and provide content on the Internet, both creating and posting electronic products and using the Internet as a communication and promotional tool for their print publishing activities.

· BiblioBytes is a private, profit-seeking enterprise that uses the World Wide Web (the "Web") to provide information about and to sell electronic books. BiblioBytes offers titles in a variety of genres, including romance, erotica, classics, adventure, and horror.

· Magazine Publishers of America ("MPA") is a national association of publishers of consumer magazines. MPA's members publish magazines in print form, but are also beginning to offer publications in electronic formats available to the public on the Internet or through online service providers.

· Interactive Digital Software Association ("IDSA") is a non-profit trade association of United States publishers of entertainment software. IDSA has many members who both sell their software in retail outlets and make their entertainment software available to the public on the Internet for demonstration, purchase, and play.

· Public Access Networks Corporation ("Panix") is an Internet service provider serving subscribers located in the New York area. Panix also hosts various organizational Web pages, assists its subscribers in creating individual Web pages, and hosts online discussion groups and chat rooms.

· ECHO is a for-profit Internet service provider that offers a "virtual salon" to Internet users. ECHO and its subscribers provide content on the Internet through the posting of Web sites, including personal home pages, and through over 50 discussion groups oriented to subscribers' interests.

· New York City Net ("NYC Net") is a for-profit Internet service provider catering primarily to lesbians and gay men in the New York area. NYC Net provides access services and content specifically oriented to gay and lesbian interests, including a large number of online discussion groups and chat rooms.

· Art on the Net is a non-profit organization with an international artist site ("art.net") on the Web. Art on the Net assists over 110 artists from all over the world in maintaining online studios.

· Peacefire is an organization whose membership consists primarily of minors. It was formed to protect the rights of citizens under the age of 18 to use the Internet. Peacefire's members use the Internet to communicate and access a wide variety of information. Peacefire's founder points out in his Declaration that Internet access is particularly important to those members who are too young to drive and might otherwise be unable to view materials from museums, libraries, and other institutions to which their families are unwilling to transport them. (See Declaration of Bennett Haselton, sworn to on March 12, 1997, at p. 4.

· American Civil Liberties Union ("ACLU") is a national civil rights organization. The ACLU maintains a Web site on which it posts civil liberties information and resources, including material about arts censorship, obscenity laws, discrimination against lesbians and gays, and reproductive choice. In addition, the ACLU hosts unmoderated online discussion groups that allow citizens to discuss and debate a variety of civil liberties issues.

Defendants in this case are the Governor and the Attorney General of New York. Defendants have raised the question of whether an injunction against those parties would also bind the sixty-two District Attorneys in New York who would actually be mounting prosecutions against alleged violators of the Act. Fed. R. Civ. P. 65(d) provides:

> Every order granting an injunction . . . is binding only upon the parties to the action, their officers, agents, servants, employees, and attorneys, and upon those persons in active concert or participation with them who receive actual notice of the order by personal service or otherwise.

Thus, parties such as the local District Attorneys who "participate" in the enjoined activities with defendants and who have actual notice of the injunction would be bound. See American Booksellers v. Webb, 590 F. Supp. 677, 693-94 (N.D. Ga. 1984) (holding that an injunction against the Attorney General also binds state law enforcement officials who might seek to enforce the challenged Act); see also United Transportation Union v. Long Island RR Co., 634 F.2d 19, 22 (2d Cir. 1980) (binding non-party Attorney General to the terms of an injunction against the defendants because Attorney General "undoubtedly had knowledge of the instant action and could have participated therein had he chosen to do so"), rev'd on other grounds, 455 U.S. 678 (1982). Thus, a preliminary injunction would effectively bar enforcement of the Act whether the prosecution happened to be brought directly by the Attorney General's office or by one of the individual District Attorneys.

II. The Challenged Statute

The Act in question amended N.Y. Penal Law § 235.21 by adding a new subdivision. The amendment makes it a crime for an individual:

> Knowing the character and content of the communication which, in whole or in part, depicts actual or simulated nudity, sexual conduct or sado-masochistic abuse, and which is harmful to minors, [to] intentionally use[] any computer communication system allowing the input, output, examination or transfer, of computer data or computer programs from one computer to another, to initiate or engage in such communication with a person who is a minor.

Violation of the Act is a Class E felony, punishable by one to four years of incarceration. The Act applies to both commercial and non-commercial disseminations of material.

Section 235.20(6) defines "harmful to minors" as:

that quality of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sado- masochistic abuse, when it:

(a) Considered as a whole, appeals to the prurient interest in sex of minors; an

(b) Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and

(c) Considered as a whole, lacks serious literary, artistic, political and scientific value for minors.

N.Y. Penal Law § 235.20 (6).

The statute provides six defenses to liability. First, Section 235.15(1) provides the following affirmative defense to prosecution under § 235.21(3):

> In any prosecution for obscenity, or disseminating indecent material to minors in the second degree in violation of subdivision three of section 235.21 of this article, it is an affirmative defense that the persons to whom the allegedly obscene or indecent material was disseminated, or the audience to an allegedly obscene performance, consisted of persons or institutions having scientific, educational, governmental or other similar justification for possessing, disseminating or viewing the same.

The statute further provides four regular defenses to prosecution:

> (a) The defendant made a reasonable effort to ascertain the true age of the minor and was unable to do so as a result of the actions taken by the minor; or
>
> (b) The defendant has taken, in good faith, reasonable, effective and appropriate actions under the circumstances to restrict or prevent access by minors to materials specified in such subdivision, which may involve any appropriate measures to restrict minors from access to such communications, including any method which is feasible under available technology; or
>
> (c) The defendant has restricted access to such materials by requiring use of a verified credit card, debit account, adult access code or adult personal identification number; or
>
> (d) The defendant has in good faith established a mechanism such that the labelling, segregation or other mechanism enables such material to be ~~automatically blocked or screened by software or other capabilities reasonably~~

> automatically blocked or screened by software or other capabilities reasonably available to responsible adults wishing to effect such blocking or screening and the defendant has not otherwise solicited minors not subject to such screening or blocking capabilities to access that material or circumvent any such screening or blocking.

N.Y. Penal Law § 235.23(3). And, finally, Section 235.24 provides that no individual shall be held liable:

> [S]olely for providing access or connection to or from a facility, system, or network not under that person's control, including transmission, downloading, intermediate storage, access software, or other related capabilities that are incidental to providing such access or connection that do not include the creation of the content of the communication.

N.Y. Penal Law § 235.24. Exceptions to this defense for conspirators or co-owners and an additional employer liability defense are set forth in Section 235.24(1)(a)-(b) and (2).

III. The Internet[2]

The Internet is a decentralized, global communications medium linking people, institutions, corporations, and governments all across the world. ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa.), prob. juris. noted, 117 S. Ct. 554 (1996), argued, March 19, 1997; Shea v. Reno, 930 F. Supp. 916 (S.D.N.Y. 1996), argued, March 19, 1997. The nature of the Internet makes it very difficult, if not impossible, to determine its size at any given moment. Undoubtedly, however, the Internet has experienced extraordinary growth in recent years. In 1981, fewer than 300 computers were linked to the Internet; in 1989, the number stood at fewer than 90,000 computers. By 1993, over 1,000,000 computers were linked. Today, over 9,400,000 host computers worldwide, 60% of them located in the United States, are linked to the Internet. This count does not include users who access the Internet via modem link-up from their personal computers. As many as 40 million people worldwide currently enjoy access to the Internet's rich variety of resources, and that number is expected to grow to 200 million by the year 1999.

The Internet is a network of networks -- a decentralized, self-maintaining series of redundant links among computers and computer networks, capable of rapidly transmitting communications without direct human involvement or control. No organization or entity controls the Internet; in fact, the chaotic, random structure of the Internet precludes any exercise of such control.

The information available on the Internet is "as diverse as human thought," ACLU, 929 F. Supp. at 842. Every facet of art, literature, music, news, and debate is represented. There can be no question that the overwhelming variety of available information includes some sexually explicit materials. Sexually-oriented content is, however, not "the primary type of content on this new medium." Id.

Individuals obtain access to the Internet via a number of avenues. Students and faculty often obtain access via their educational institutions; similarly, some corporations provide their employees with direct or modem access to the Internet. Individuals in some communities can access the Internet via a community network or a local library that provides direct or modem access to library patrons. Storefront "computer coffee shops" offer another option, serving up access to cyberspace accompanied by coffee and snacks for a small hourly fee. "Internet service providers" typically offer modem telephone access to a computer or computer network linked to the Internet. Many such providers -- including plaintiffs Panix, Echo, and NYC NET -- are commercial entities offering Internet access for a monthly or hourly fee. Another common way for individuals to access the Internet is through one of the major national commercial "online services" such as America Online, Compuserve, the Microsoft Network, or Prodigy, which collectively service almost twelve million individual

America, and the Medical Library Association. "These links from one computer to another, from one document to another across the Internet, are what unify the Web into a single body of knowledge, and what makes the Web unique." Id. at 836-37.

Regardless of the aspect of the Internet they are using, Internet users have no way to determine the characteristics of their audience that are salient under the New York Act -- age and geographic location. In fact, in online communications through newsgroups, mailing lists, chat rooms, and the Web, the user has no way to determine with certainty that any particular person has accessed the user's speech. "Once a provider posts content on the Internet, it is available to all other Internet users worldwide." Id. at 844. A speaker thus has no way of knowing the location of the recipient of his or her communication. As the poet said, "I shot an arrow into the air; it fell to the earth I know not where."

This highly simplified description of the Internet is not intended to minimize its marvels. While no one should lose sight of the inventiveness that has made this complex of resources available to just about anyone, the innovativeness of the technology does not preclude the application of traditional legal principles -- provided that those principles are adaptable to cyberspace. In the present case, as discussed more fully below, the Internet fits easily within the parameters of interests traditionally protected by the Commerce Clause. The New York Act represents an unconstitutional intrusion into interstate commerce; plaintiffs are therefore entitled to the preliminary injunction that they seek.

DISCUSSION

I. Standard Applicable to a Preliminary Injunction

To demonstrate their entitlement to a preliminary injunction, plaintiffs must show (a) that they will suffer irreparable harm and (b) either (i) a likelihood of success on the merits or (ii) sufficiently serious questions going to the merits to make them a fair ground for litigation[3] and a balance of hardships tipping decidedly in the plaintiffs' favor. Paulsen v. County of Nassau, 925 F.2d 65, 68 (2d Cir. 1991); Streetwatch v. National R.R. Passenger Corp., 875 F. Supp. 1055, 1058 (S.D.N.Y. 1995). In the present case, as discussed more fully below, plaintiffs have amply demonstrated the likelihood of their successful prosecution of their claim that the Act violates the Commerce Clause because it seeks to regulate communications occurring wholly outside New York, imposes a burden on interstate commerce that is disproportionate to the local benefits it is likely to engender, and subjects plaintiffs, as well as other Internet users, to inconsistent state obligations. See Healy v. Beer Institute, 491 U.S. 324, 332 (1989); Pike v. Bruce Church. Inc., 397 U.S. 137, 142 (1970); Southern Pac. Co. v. Arizona ex rel. Sullivan, 325 U.S. 761, 767 (1945).

Plaintiffs have also shown that they face irreparable injury in the absence of an injunction. Irreparable injury means "the kind of injury for which money cannot compensate," Sperry Int'l Trade. Inc. v. Government of Israel, 670 F.2d 8, 12 (2d Cir. 1982), and which is "neither remote nor speculative, but actual and imminent." Tucker Anthony Realty Corp. v. Schlesinger, 888 F.2d 969, 975 (2d Cir. 1989). Deprivation of the rights guaranteed under the Commerce Clause constitutes irreparable injury. C & A Carbone. Inc. v. Town of Clarkstown, 770 F. Supp. 848, 854 (S.D.N.Y. 1991) (holding that a local waste disposal law caused irreparable injury to the plaintiffs' rights under the Commerce Clause). Thus, by demonstrating that the Act threatens their rights under the Commerce Clause, as will be discussed more fully below, the plaintiffs have shown both irreparable injury and a likelihood of success on the merits.

II. Federalism and the Internet: The Commerce Clause

The borderless world of the Internet raises profound questions concerning the relationship among the several states and the relationship of the federal government to each state, questions that go to the heart of "our federalism." See Youncer v. Harris, 401 U.S. 37, 44 (1971) ("[O]ne familiar with the profound debates that ushered our Federal Constitution into

existence is bound to respect those who remain loyal to the ideals and dreams of 'Our Federalism.' The concept does not mean blind deference to 'States' Rights' any more than it means centralization of control over every important issue in our National Government and its courts. The Framers rejected both these courses.") The Act at issue in the present case is only one of many efforts by state legislators to control the chaotic environment of the Internet. For example, the Georgia legislature has enacted a recent law prohibiting Internet users from "falsely identifying" themselves online. Ga. Stat. 16-9-9.1. Similar legislation is pending in California. California Senate Bill SB-1533 (1996); see also Ilana DeBare, State Trademark Bill Ignites Net Turmoil, The Sacramento Bee, March 2, 1991, at F1. Texas and Florida have concluded that law firm web pages (apparently including those of out of state firms) are subject to the rules of professional conduct applicable to attorney advertising. See Texas Bar Advertising Comm., Interpretive Comment on Attorney Internet Advertising (1996); see also Texans Against Censorship v. State Bar of Texas, 888 F. Supp. 1328, 1369-70 (E.D. Tex. 1995) (discussing applicability of Texas lawyers advertising regulation to the Internet), aff'd, 100 F.3d 953 (5th Cir. 1996); Ethics Update, Fla. Bar News, January 1, 1996. Further, states have adopted widely varying approaches in the application of general laws to communications taking place over the Internet. Minnesota has aggressively pursued out-of-state advertisers and service providers who reach Minnesotans via the Internet; Illinois has also been assertive in using existing laws to reach out-of-state actors whose connection to Illinois occurs only by virtue of an Internet communication. See Mark Eckenwiler, States Get Entangled in the Web, Legal Times, Jan. 22, 1996, at S35, S37. Florida has taken the opposite route, declining to venture into online law enforcement until various legal issues (including, perhaps, the one discussed in the present opinion) have been determined. Id. at S37.[4]

The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet. The menace of inconsistent state regulation invites analysis under the Commerce Clause of the Constitution, because that clause represented the framers' reaction to overreaching by the individual states that might jeopardize the growth of the nation -- and in particular, the national infrastructure of communications and trade -- as a whole. See Quill Corp. v. North Dakota, 504 U.S. 298, 312 (1992) ("Under the Articles of Confederation, state taxes and duties hindered and suppressed interstate commerce; the Framers intended the Commerce Clause as a cure for these structural ills."); see also The Federalist Nos. 7, 11 (A. Hamilton).

The Commerce Clause is more than an affirmative grant of power to Congress. As long ago as 1824, Justice Johnson in his concurring opinion in Gibbons v. Ogden, 9 Wheat. 1, 231-32, 239 (1824), recognized that the Commerce Clause has a negative sweep as well. In what commentators have come to term its negative or "dormant" aspect, the Commerce Clause restricts the individual states' interference with the flow of interstate commerce in two ways. The Clause prohibits discrimination aimed directly at interstate commerce, see, e.g., Philadelphia v. New Jersey, 437 U.S. 617 (1978), and bars state regulations that, although facially nondiscriminatory, unduly burden interstate commerce, see. e.g., Kassel v. Consolidated Freiqhtways Corp. of Del., 450 U.S. 662 (1981). Moreover, courts have long held that state regulation of those aspects of commerce that by their unique nature demand cohesive national treatment is offensive to the Commerce Clause. See e.g., Wabash St. L. & P. Rv. Co. v. Illinois, 118 U.S. 557 (1887) (holding railroad rates exempt from state regulation).

Thus, as will be discussed in more detail below, the New York Act is concerned with interstate commerce and contravenes the Commerce Clause for three reasons. First, the Act represents an unconstitutional projection of New York law into conduct that occurs wholly outside New York. Second, the Act is invalid because although protecting children from indecent material is a legitimate and indisputably worthy subject of state legislation, the

burdens on interstate commerce resulting from the Act clearly exceed any local benefit derived from it. Finally, the Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether. Thus, the Commerce Clause ordains that only Congress can legislate in this area, subject, of course, to whatever limitations other provisions of the Constitution (such as the First Amendment) may require.

A. The Act Concerns Interstate Commerce

At oral argument, the defendants advanced the theory that the Act is aimed solely at intrastate conduct. This argument is unsupportable in light of the text of the statute itself, its legislative history, and the reality of Internet communications. The section in question contains no such limitation; it reads:

> A person is guilty of disseminating indecent material to minors in the second degree when:
> ....
>
> > (3) Knowing the character and content of the communication which, in whole or in part, depicts actual or simulated nudity, sexual conduct or sado masochistic abuse, and which is harmful to minors, he intentionally uses any computer communication system allowing the input, output, examination or transfer, of computer data or computer programs from one computer to another, to initiate or engage in such communication with a person who is a minor.

N.Y. Penal Law § 235.21(3) (McKinney's 1997). Section 235.20, which contains the definitions applicable to the challenged portion of the Act, does not import any restriction that the criminal communication must take place entirely within the State of New York. By its terms, the Act applies to any communication, intrastate or interstate, that fits within the prohibition and over which New York has the capacity to exercise criminal jurisdiction. See Boyd v. Meachum, 77 F.3d 60, 65 (2d Cir. 1996) (holding that a criminal court "has personal jurisdiction over any party who appears before it, regardless of how his appearance was obtained"), cert. denied, 117 S. Ct. 114 (1996); see also United States v. Lussier, 929 F.2d 25, 27 (1st Cir. 1991); United States v. Stuart, 689 F.2d 759, 762 (8th Cir. 1982), cert. denied, 460 U.S. 1037 (1983).

Further, the legislative history of the Act clearly evidences the legislators' understanding and intent that the Act would apply to communications between New Yorkers and parties outside the State, despite occasional glib references to the Act's "intrastate" applicability. The New York State Senate Introducer's Memorandum in Support of the Act contains a paragraph under the subtitle, "Justification," which states:

> Law enforcement agencies around the nation are becoming increasingly alarmed at the growing use of computer networks and other communications by pedophiles. As one observer noted, "perverts are moving from the playground to the internet." Several cases have come to light wherein a pedophile has traveled clear across the country to have sexual relations with a minor initially contacted and engaged through various computer networks.

(Affidavit of James Hershler, Exh. D) (emphasis added). A letter from the Bill's sponsor to Governor Pataki characterized sexually-infused Internet communications between adults and minors as "long-distance, high-tech sexual abuse." (See Letter dated July 11, 1996 from William Sears to Governor Pataki, designated page 3 in the Bill Jacket, Hershler Aff., Exh. A). Jeanine Pirro, the Westchester County District Attorney, wrote a letter to Governor Pataki dated February 13, 1996 that similarly reflects the expectations of the Act's proponents that it would apply to interstate communications. Ms. Pirro's letter states:

proponents that it would apply to interstate communications. Ms. Pirro's letter states:

> This bill was proposed partly in response to a Westchester County case wherein an adult male resident of Seattle, Washington, [one Alan Paul Barlow,] communicated about sexually explicit matters by computer with a thirteen year old girl over several months.

(Hershler Aff., Exh. F); see also John Heileman, The Crusader, The New Yorker, February 24 and March 3, 1997 (detailing Ms. Pirro's "crusade" to achieve the passage of the Act in the aftermath of the Barlow incident).[5] Ms. Pirro's references to this incident, known as the Barlow case, are echoed throughout defendants' memorandum of law. (See Defendants' Memorandum of Law in Opposition to Preliminary Injunction, pp. 15, 16, 17-18). Obviously, however, the Act would be completely ineffective in forestalling a pedophile like Barlow if it applied only to purely intrastate communications.

The conclusion that the Act must apply to interstate as well as intrastate communications receives perhaps its strongest support from the nature of the Internet itself. The Internet is wholly insensitive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources they access. Internet protocols were designed to ignore rather than document geographic location; while computers on the network do have "addresses," they are logical addresses on the network rather than geographic addresses in real space. The majority of Internet addresses contain no geographic clues and, even where an Internet address provides such a clue, it may be misleading. For example, in his article, Federalism in Cyberspace, 28 Conn. L. Rev. 1095, 1112 (1996), Professor Dan Burk described how he uses Seton Hall University's computer system to access the Internet, providing anyone who communicates with him (and is aware of Seton Hall's locale) a hint that he is in New Jersey. However, Professor Burk also has a guest account at a university in California which he continues to use even when he is in New Jersey; any clue derived from the California university's name within the Internet address would therefore be deceptive. In a similar vein, Ms. Kovacs testified that as she was using her computer to give an in-court demonstration of various Internet applications, she received an e-mail from a colleague who believed she was sending the message to Cincinnati, Ohio (where Ms. Kovacs is normally located); in fact, Ms. Kovacs was in New York and received the message here. (4/4/97 Tr., p. 61).

Moreover, no aspect of the Internet can feasibly be closed off to users from another state. An internet user who posts a Web page cannot prevent New Yorkers or Oklahomans or Iowans from accessing that page and will not even know from what state visitors to that site hail. Nor can a participant in a chat room prevent other participants from a particular state from joining the conversation. Someone who uses a mail exploder is similarly unaware of the precise contours of the mailing list that will ultimately determine the recipients of his or her message, because users can add or remove their names from a mailing list automatically. Thus, a person could choose a list believed not to include any New Yorkers, but an after-added New Yorker would still receive the message.[6]

E-mail, because it is a one-to-one messaging system, stands on a slightly different footing than the other aspects of the Internet. Even in the context of e-mail, however, a message from one New Yorker to another New Yorker may well pass through a number of states en route. The Internet is, as described above, a redundant series of linked computers. Thus, a message from an Internet user sitting at a computer in New York may travel via one or more other states before reaching a recipient who is also sitting at a terminal in New York.

The system is further complicated by two Internet practices: packet switching and caching. "Packet switching" protocols subdivide individual messages into smaller packets that are then sent independently to the destination, where they are automatically reassembled by the receiving computer. If computers along the route become overloaded, packets may be rerouted to computers with greater capacity. A single message may -- but does not always -- travel several different pathways before reaching the receiving computer. "Caching" is the

travel several different pathways before reaching the receiving computer. "Caching" is the Internet practice of storing partial or complete duplicates of materials from frequently accessed sites to avoid repeatedly requesting copies from the original server. The recipient has no means of distinguishing between the cached materials and the original. Thus, the user may be accessing materials at the original site, or he may be accessing copies of those materials cached on a different machine located anywhere in the world.

The New York Act, therefore, cannot effectively be limited to purely intrastate communications over the Internet because no such communications exist. No user could reliably restrict her communications only to New York recipients. Moreover, no user could avoid liability under the New York Act simply by directing his or her communications elsewhere, given that there is no feasible way to preclude New Yorkers from accessing a Web site, receiving a mail exploder message or a newsgroup posting, or participating in a chat room. Similarly, a user has no way to ensure that an e-mail does not pass through New York even if the ultimate recipient is not located there, or that a message never leaves New York even if both sender and recipient are located there.

This conclusion receives further support from the unchallenged testimony that plaintiffs introduced in the form of declarations. For example, Stacy Horn, the president of ECHO, an electronic cultural salon, testified that "[c]onference participants do not know, and have no way to determine, the . . . geographic location of other participants." (Decl. of Stacy Horn, sworn to on March 12, 1997, at p. 6). Oren Teicher, the President of the American Booksellers Foundation for Free Expression, indicated that:

> Much of the Internet use by booksellers is interstate in nature. For example, any bookseller's Web page can be accessed by Internet users not only throughout the United States, but throughout the world. Similarly, ABFFE members from across the country communicate with one another as well as Internet users across the country via e-mail. Moreover, ABFFE users cannot effectively prevent their Web sites or discussion groups from being accessed by New York users.

(Decl. of Oren Teicher, sworn to on March 26, 1997, at p. 4). Lawrence J. Kaufman, the Vice President of the Magazine Publishers of America, Inc., a trade association for the consumer magazine industry, noted that "On-line users anywhere in the world can access the content provided by MPA members on the Web and via e-mail. These members cannot effectively prevent their Web sites from being accessed by New York users." (Decl. of Lawrence J. Kaufman, sworn to on March 26, 1997, at p.2).

The Act is therefore necessarily concerned with interstate communications. See Virginia v. American Booksellers Assn., Inc., 484 U.S. 383, 397 (1988) (holding that only if a statute is "readily susceptible" to a narrowing construction will the court apply such a construction to save an otherwise unconstitutional law). The next question that requires an answer as a threshold matter is whether the types of communication involved constitute "commerce" within the meaning of the Clause.

The definition of commerce in the Supreme Court's decisions has been notably broad. Most recently, in Camps Newfound Owatonna, Inc. v. Town of Harrison, Maine, 1997 WL 255351 (May 19, 1997), the Court rejected defendant's arguments that the Commerce Clause was inapplicable to a discriminatory real estate tax deduction, either because "campers are not 'articles of commerce'" or because the plaintiff camp's "product is delivered and 'consumed' entirely within Maine." Id. at *5. In the past, the Court has held that interstate commerce is affected by private race discrimination that limited access to a hotel and thereby impeded interstate commerce in the form of travel. Heart of Atlanta Motel, Inc. v. United States, 379 U.S. 241, 244, 258 (1964).

In the present case, the parties have stipulated that:

> The Internet is not exclusively, or even primarily, a means of commercial communication. Many commercial entities maintain Web sites to inform potential consumers about their goods and services, or to solicit purchases, but many other Web sites exist solely for the dissemination of non-commercial information. The other forms of Internet communication -- e-mail, bulletin boards, newsgroups, and chat rooms -- frequently have non-commercial goals. For the economic and technical reasons set forth in the following paragraphs, the Internet is an especially attractive means for not-for-profit entities or public interest groups to reach their desired audiences. There are examples in the plaintiffs' affidavits of some of the non-commercial uses that the Internet serves. Plaintiff Peacefire offers information on its Internet site regarding the rights of minors on the Internet. Plaintiff Art on the Net allows artists to post their works on the World Wide Web. Plaintiff American Civil Liberties Union offers information on civil liberties issues.

(Joint Stipulation of Facts, ¶ 79). This stipulation, however inartfully worded, cannot insulate the statute at issue from Commerce Clause scrutiny. The non-profit nature of certain entities that use the Internet or of certain transactions that take place over the Internet does not take the Internet outside the Commerce Clause. See Camps Newfound, at *6; Hughes v. Oklahoma, 441 U.S. 322, 326 n.2 (1979); Philadelphia v. New Jersey, 437 U.S. 617, 621-23 (1978).

The Supreme Court has expressly held that the dormant commerce clause is applicable to activities undertaken without a profit motive. In Edwards v. California, 314 U.S. 160 (1941), the Court examined the constitutionality of a California statute prohibiting the transport of indigent people into the state. The Court struck the statute as violative of the dormant Commerce Clause, reasoning that "the transportation of persons is 'commerce,'" and that the California law at issue raised an "unconstitutional barrier to that commerce." Id. at 172-73. In making its threshold determination, the Court emphasized that "[i]t is immaterial whether or not the transportation is commercial in character." Id. at 172, n.l; see also Caminetti v. United States, 242 U.S. 470, 491 (1917); Hoke v. United States, 227 U.S. 308, 320 (1913).

Commercial use of the Internet, moreover, is a growing phenomenon. See, e.g., Don Clark, Disney Launching Children's Web Site Only on Microsoft's On-Line Service, Wall St. Journal, March 31, 1997 (describing Disney's efforts to create and market a fee-based Web service); see also Andrew Bowser, Advertising on the Net, New Orleans Citybusiness, March 6, 1995; John Casey, Growing Potential of World Wide Web, Business & Finance, The Irish Times, June 3, 1996. In addition, many of those users who are communicating for private, noncommercial purposes are nonetheless participants in interstate commerce by virtue of their Internet consumption. Many users obtain access to the Internet by means of an on-line service provider, such as America Online, which charges a fee for its services. "Internet service providers," including plaintiffs Panix, Echo, and NYC NET, also offer Internet access for a monthly or hourly fee. Patrons of storefront "computer coffee shops," such as New York's own CyberCafe, similarly pay for their access to the Internist, in addition to partaking of food and beverages sold by the cafe. Dial-in bulletin board systems often charge a fee for access. See Katzenbach v. McClung, 379 U.S. 294, 300-301 (1964) (holding that an entity that purchases goods used in the provision of its services from interstate sources is an actor in interstate commerce even in connection with the provision of services within a single state).

The courts have long recognized that railroads, trucks, and highways are themselves "instruments of commerce," because they serve as conduits for the transport of products and services. See Kassel v. Consolidated Freightways Corp., 450 U.S. 662 (1981); Southern Pacific Co. v. Arizona, 32S U.S. 761, 780 (1945). The Internet is more than a means of communication; it also serves as a conduit for transporting digitized goods, including software, data, music, graphics, and videos which can be downloaded from the provider's site to the Internet user's computer. For example, plaintiff BiblioBytes and members of

site to the Internet user's computer. For example, plaintiff BiblioBytes and members of plaintiff IDSA both sell and deliver their products over the Internet.

The inescapable conclusion is that the Internet represents an instrument of interstate commerce, albeit an innovative one; the novelty of the technology should not obscure the fact that regulation of the Internet impels traditional Commerce Clause considerations. The New York Act is therefore closely concerned with interstate commerce, and scrutiny of the Act under the Commerce Clause is entirely appropriate. As discussed in the following sections, the Act cannot survive such scrutiny, because it places an undue burden on interstate traffic, whether that traffic be in goods, services, or ideas.

B. New York Has Overreached by Enacting a Law That Seeks To Regulate Conduct Occurring Outside its Borders

The interdiction against direct interference with interstate commerce by state legislative overreaching is apparent in a number of the Supreme Court's decisions. In Baldwin v. G.A.F. Seelig Inc., 294 U.S. 511, 521 (1935), for example, Justice Cardozo authored an opinion enjoining enforcement of a law that prohibited a dealer from selling within New York milk purchased from the producer in Vermont at less than the minimum price fixed for milk produced in New York. Justice Cardozo sternly admonished, "New York has no power to project its legislation into Vermont by regulating the price to be paid in that state for milk," finding that "[s]uch a power, if exerted, [would] set a barrier to traffic between one state and another as effective as if customs duties, equal to the price differential, had been laid upon the thing transported." Id.

The Court has more recently confirmed that the Commerce Clause precludes a state from enacting legislation that has the practical effect of exporting that state's domestic policies. In Edgar v. MITE, 457 U.S. 624 (1982), the Court examined the constitutionality of an Illinois anti-takeover statute that required a tender offeror to notify the Secretary of State and the target company of its intent to make a tender offer and the terms of the offer 20 days before the offer became effective. During the twenty-day period, the offeror was barred from communicating its offer to the shareholders, but the target company was free to disseminate information to its shareholders concerning the impending offer. Id. at 633. The statute defined "target company" as a corporation of which Illinois shareholders own 10% of the class of securities subject to the takeover offer, or for which any two of the following conditions are met: the corporation has its principal office in Illinois, is organized under Illinois law, or has at least 10% of its stated capital and paid-in surplus within Illinois. Id. at 625. The Court acknowledged that states traditionally retained the power to regulate intrastate securities transactions by enacting "blue-sky laws." Id. at 641. Nonetheless, the Court asserted that "[t]he Illinois Act differs substantially from state blue-sky laws in that it directly regulates transactions which take place across state lines, even if wholly outside the State of Illinois." Id. In striking the law as violative of the Commerce Clause, the Court found particularly egregious the fact that the Illinois law on its face would apply to a transaction that would not affect a single Illinois shareholder if a corporation fit within the definition of a "target company." Id. at 642. The Court concluded "the Illinois statute is a direct restraint on interstate commerce and has a sweeping extraterritorial effect," because the statute would prevent a tender offeror from communicating its offer to shareholders both within and outside Illinois. Acceptance of the offer by any of the shareholders would result in interstate transactions; the Illinois statute effectively stifled such transactions during the waiting period and thereby disrupted prospective interstate commerce. Under the Commerce Clause, the projection of these extraterritorial "practical effect[s]," regardless of the legislators' intentions, "'exceeded the inherent limits of the State's power.'" Id. at 642-43 (quoting Shaffer v. Heitner, 433 U.S. 186, 197 (1977)).

In the present case, a number of witnesses testified to the chill that they felt as a result of the enactment of the New York statute; these witnesses refrained from engaging in particular types of interstate commerce. In particular, I note the testimony of Rudolf Kinsky, an artist with a virtual studio on Art on the Net's Website. Mr. Kinsky testified that he removed

several images from his virtual studio because he feared prosecution under the New York Act. (4/7/97 Tr., at 231-35). As described above, no Web siteholder is able to close his site to New Yorkers. Thus, even if Mr. Kinsky were located in California and wanted to display his work to a prospective purchaser in Oregon, he could not employ his virtual studio to do so without risking prosecution under the New York law.

Oren Teicher, the President of the American Booksellers Foundation for Free Expression, similarly testified to the stifling effects that the Act will have on prospective interstate commerce in books, stating that:

> The Internet is an important source of interstate business for ABFFE members . . . [B]ooksellers conduct business over the Internet in a variety of ways. If the Act is not enjoined and ABFFE members are forced to self-censor rather than be subject to criminal liability, they will suffer immeasurable injury because they will lose significant sales and goodwill generated by their use of the Internet with respect to both censored and noncensored materials and resources. If a bookstore must self-censor certain books, it loses the profits from the sale of those particular books generated from the books' listing on the booksellers' Web sites. In addition, the bookstore will lose even more business because it will appear that the bookstore has an incomplete or inadequate listing of books in its inventory and Internet users will choose to buy their books elsewhere.

(Teicher Decl., pp. 4-5). Lawrence Kaufman, the Vice President of the Magazine Publishers of America, also testified to the interstate nature of the business conducted by MPA over the Internet and to the loss of sales and goodwill that MPA members will suffer if forced to self-censor in order to avoid criminal liability under the Act. In particular, Mr. Kaufman noted that Playboy magazine, an MPA member, occasionally posts electronic versions or excerpts from its magazines that might fall within the Act's prohibition, presumably in an effort to attract new readership and subscribers. (Kaufman Decl. pp. 2-3). Edgar teaches that for New York to attempt to strangle prospective interstate transactions between parties from states other than New York by this means offends the Commerce Clause.

The "extraterritoriality" analysis of the Edgar opinion commanded only a plurality of the Court. Later majority holdings, however, expressly adopted the underlying principles on which Justice White relied in Edgar. See Healy v. The Beer Institute, 491 U.S. 324 (1989); Brown-Forman Distillers Corp. v New York State Liquor Authority, 476 U.S. 573 (1986). In Healy the Court assessed the constitutionality of a Connecticut statute that required that out-of-state beer shippers affirm that their prices were no higher than the prices being charged in the bordering states at the time of the affirmation. The Court derived three guiding principles from its prior cases. First, the Court emphasized that the "'Commerce Clause . . . precludes the application of a state statute to commerce that takes place wholly outside the State's borders, whether or not the commerce has effects within the state.'" Healy, 491 U.S. at 336 totting Edgar, 457 U.S. at 642-43; Brown-Forman, 476 U.S. at 581-583). Second, the Court instructed that "a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State." Id. citing Brown-Forman, 476 U.S. at 579). Finally, "the practical effect of the statute must be evaluated not only by considering the consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other States and what effect would arise if not one, but many or every, State adopted similar legislation. Generally speaking, the Commerce Clause protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State." Id.; cf. CTS Corp. v. Dynamics Corn. of America, 481 U.S. 69, 88-89 (1987).

Applying these principles to the Connecticut price affirmation statute, the Court held that the statute had the undeniable and impermissible effect of controlling commercial activity occurring wholly outside Connecticut. In particular, the Court examined the practical impact of the statute, in light of the regulations prevailing in the neighboring states of Massachusetts and New York and determined that the affirmation law, when taken in conjunction with the laws that had been or might be enacted in neighboring states, created "just the kind of competing and interlocking local economic regulation that the Commerce Clause was meant to preclude." Healy, 491 U.S. at 337.

The Edgar/Healy extraterritoriality analysis rests on the premise that the Commerce Clause has two aspects: it subordinates each state's authority over interstate commerce to the federal power of regulation (a vertical limitation), and it embodies a principle of comity that mandates that one state not expand its regulatory powers in a manner that encroaches upon the sovereignty of its fellow states (a horizontal limitation). The Court most recently recognized this duality in BMW of North America, Inc. v. Gore, 116 S. Ct. 1589 (1996). In a seminal case concerning an American's most precious possession (if not his most precious rights), a BMW purchaser in Alabama sued after discovering that his new BMW had been repainted prior to sale, alleging that the failure to disclose the repainting constituted fraud under Alabama law. Although the difference caused by the repainting was apparently imperceptible to the layperson, when the purchaser brought his car to "Slick Finish," an independent detailer, to make it look "snazzier than it normally would appear," 646 So.2d 619, 621 (Ala. 1994), Mr. Slick, the aptly yclept proprietor, detected evidence that the car had been repainted. The plaintiff alleged that he had suffered $4,000 in actual damages, relying on the testimony of a former BMW dealer who estimated that the value of a repainted BMW was approximately 10% less than one that was "showroom new." Plaintiff further argued that a punitive damage award of $4 million was an appropriate penalty in light of evidence he introduced that BMW had sold 983 refinished cars as new, including 14 in Alabama.

At trial, BMW acknowledged that it had adopted a nationwide policy of disclosing predelivery repairs only when the cost of the repairs exceeded 3% of the car's suggested retail price. The jury returned a verdict finding BMW liable for compensatory damages of $4,000 and punitive damages of $4 million, apparently calculated by multiplying the number of sales in all states of refinished cars by $4,000. BMW filed a post-trial motion to set aside the punitive damages award, contending that its nondisclosure policy was consistent with the laws of 25 states defining the disclosure obligations of automobile manufacturers; BMW asserted that the punitive damages were excessive because they were computed on the basis of sales that took place in jurisdictions where its conduct was perfectly legal.

The Supreme Court agreed. The Court indicated that while Congress could enact a law requiring full disclosure of every presale repair to an automobile, no single state could impose such a policy nationwide by imposing economic sanctions aimed at changing the conduct of a tortfeasor in other states. Id. at 1596. Speaking emphatically of the need to confine state legislation to its proper constitutional sphere, the Court stated:

> [O]ne State's power to impose burdens on the interstate market for automobiles is not only subordinate to the federal power over interstate commerce, Gibbons v. Ogden, 9 Wheat. 1, 194-96, 6 L.Ed. 23 (1824), but is also constrained by the need to respect the interests of other States, see, e.g., Healy v. Beer Institute, 491 U.S. 324, 335-36, 109 S. Ct. 2491, 2498-99, 105 L.Ed. 275 (1989) (the Constitution has a "special concern both with the maintenance of a national economic union unfettered by state-imposed limitations on interstate commerce and with the autonomy of the individual States within their respective spheres" (footnote omitted)); Edgar v. MITE Corp., 457 U.S. 624, 643, 102 S. Ct. 2629, 2641, 73 L.Ed.2d 269 (1982).

Id. The need to contain individual state overreaching thus arises not from any disrespect for

Id. The need to contain individual state overreaching thus arises not from any disrespect for the plenary authority of each state over its own internal affairs but out of a recognition that true protection of each state's respective authority is only possible when such limits are observed by all states.[7]

The nature of the Internet makes it impossible to restrict the effects of the New York Act to conduct occurring within New York. An Internet user may not intend that a message be accessible to New Yorkers, but lacks the ability to prevent New Yorkers from visiting a particular Website or viewing a particular newsgroup posting or receiving a particular mail exploder. Thus, conduct that may be legal in the state in which the user acts can subject the user to prosecution in New York and thus subordinate the user's home state's policy -- perhaps favoring freedom of expression over a more protective stance -- to New York's local concerns. See Bigelow v. Virginia, 421 U.S. 309, 824 (1975) ("A State does not acquire power or supervision over the internal affairs of another State merely because the welfare and health of its own citizens may be affected when they travel to that State."). New York has deliberately imposed its legislation on the Internet and, by doing so, projected its law into other states whose citizens use the Net. See Southern Pacific Co. v. Arizona ex ref. Sullivan, 325 U.S. 761, 774 (1945) ("If one state may regulate train lengths, so may all others, and they need not prescribe the same maximum limitation. The practical effect of [a law limiting train lengths] is to control train operations beyond the boundaries of the state exacting it because of the necessity of breaking up and reassembling long trains at the nearest terminal points before entering and after leaving the regulating state."). This encroachment upon the authority which the Constitution specifically confers upon the federal government and upon the sovereignty of New York's sister states is per se violative of the Commerce Clause.

C. The Burdens the Act Imposes on Interstate Commerce Exceed Any Local Benefit

Even if the Act were not a per se violation of the Commerce Clause by virtue of its extraterritorial effects, the Act would nonetheless be an invalid indirect regulation of interstate commerce, because the burdens it imposes on interstate commerce are excessive in relation to the local benefits it confers. The Supreme Court set forth the balancing test applicable to indirect regulations of interstate commerce in Pike v. Bruce Church, 397 U.S. 137, 142 (1970).[8] Pike requires a two fold inquiry. The first level of examination is directed at the legitimacy of the state's interest. The next, and more difficult, determination weighs the burden on interstate commerce in light of the local benefit derived from the statute.

In the present case, I accept that the protection of children against pedophilia is a quintessentially legitimate state objective -- a proposition with which I believe even the plaintiffs have expressed no quarrel. See New York v. Ferber, 458 U.S. 747, 756-57 (1982) ("It is evident beyond the need for elaboration that a State's interest in 'safeguarding the physical and psychological well-being of a minor' is 'compelling.'") (quoting Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 607 (1982)); see also Sable v. Federal Communications Commission, 492 U.S. 115, 126 (1989) ("[T]here is a compelling interest in protecting the physical and psychological well-being of minors. This interest extends to shielding minors from the influence of literature that is not obscene by adult standards."). The defendants spent considerable time in their Memorandum and at argument asserting the legitimacy of the state's interest. Even with the fullest recognition that the protection of children from sexual exploitation is an indisputably valid state goal, however, the present statute cannot survive even the lesser scrutiny to which indirect regulations of interstate commerce are subject under the Constitution. The State cannot avoid the second stage of the inquiry simply by invoking the legitimate state interest underlying the Act. See Hunt v. Washington State Apple Advertising Comm'n, 432 U.S. 333, 350 (1977) ("[A] finding that state legislation furthers matters of legitimate local concern, even in the health and consumer protection areas, does not end the inquiry."); Bibb v. Navajo Freight Lines, 359 U.S. 520, 528 (1959) (holding that "local safety measures that are nondiscriminatory [can] place an unconstitutional burden on interstate commerce"); see also Dean Milk Co. v. Madison, 340 U.S. 349, 354 (1951) (holding that permitting a state to discriminate against

Madison, 340 U.S. 349, 354 (1951) (holding that permitting a state to discriminate against interstate commerce to promote the health and safety of its citizens "would mean that the Commerce Clause of itself imposes no limitations on state action . . . save for the rare instances where a state artlessly discloses an avowed purpose to discriminate against interstate goods."); Southern Pac. Co. v. Arizona, ex rel. Sullivan, 325 U.S. 761, 779 (1945) ("The principle that, without controlling Congressional action, a state may not regulate interstate commerce so as substantially to affect its flow or deprive it of needed uniformity in its regulation is not to be avoided by 'simply invoking the convenient apologetics of the police power.'") (quoting Kansas City Southern Ry. v. Kaw Valley Drainage Dist., 233 U.S. 76, 79 (1914)).

The local benefits likely to result from the New York Act are not overwhelming. The Act can have no effect on communications originating outside the United States. As the three-judge panel that struck the federal analog of the New York Act, the Communications Decency Act, on First Amendment grounds concluded:

> [The Act] will almost certainly fail to accomplish the Government's interest in shielding children from pornography on the Internet. Nearly half of Internet communications originate outside the United States, and some percentage of that figure represents pornography. Pornography from, say, Amsterdam, will be no less appealing to a child on the Internet than pornography from New York City, and residents of Amsterdam have little incentive to comply with the [Act].

American Civil Liberties Union v. Reno, 929 F. Supp. 824, 882 (E.D. Pa. 1996). Further, in the present case, New York's prosecution of parties from out of state who have allegedly violated the Act, but whose only contact with New York occurs via the Internet, is beset with practical difficulties, even if New York is able to exercise criminal jurisdiction over such parties. The prospect of New York bounty hunters dragging pedophiles from the other 49 states into New York is not consistent with traditional concepts of comity.

Moreover, the State has espoused an interpretation of the Act that, if accepted,[9] would further undermine its effectiveness. According to defendant, the Act reaches only pictorial messages that are harmful to minors and has no impact on purely textual communications. Were this interpretation adopted, Mr. Barlow, whose conduct supposedly motivated the supporters of the Act, would escape prosecution because his messages were verbal. See The Crusader, supra, at 122 (reporting Barlow's message to New York girl as "I'm feeling really horny--I think Oscar is making a 'statement.' We both want you very much. I'm thinking about you, & he's thinking about Love Bunny & tingling like mad.")

The Act is, of course, not the only law in New York's statute books designed to protect children against sexual exploitation. The State is able to protect children through vigorous enforcement of the existing laws criminalizing obscenity and child pornography. See United States v. Thomas, 74 F.3d 701, 704-05 (6th Cir. 1995), cert. denied, 117 S. Ct. 74 (1996). Moreover, plaintiffs do not challenge the sections of the statute that criminalize the sale of obscene materials to children, over the Internet or otherwise, and prohibit adults from luring children into sexual contact by communicating with them via the Internet. See N.Y. Penal Law § 235.21(1); N.Y. Penal Law § 235.22(2). The local benefit to be derived from the challenged section of the statute is therefore confined to that narrow class of cases that does not fit within the parameters of any other law. The efficacy of the statute is further limited, as discussed above, to those cases which New York is realistically able to prosecute.

The conclusion that the New York Act has a very limited effect was bolstered by the testimony of Michael McCartney, an investigator with the New York State Attorney General's office. Mr. McCartney testified that he personally had logged over 600 hours investigating on-line criminal activity. (4/3/97 Tr., p. 12). Despite this extensive investment of time, Mr. McCartney admitted that he had investigated only two cases involving the dissemination of indecent materials to minors over the Internet that did not fall into the category of child pornography (which is, of course, subject to prosecution under other laws).

(Id., p. 36). In one case, further investigation disclosed that the e-mail conversation actually took place between two adults and thus was outside the terms of the Act. (Id.). In the second case, Mr. McCartney was never able to determine which of the people in the household that held the Internet access account was responsible for sending the messages and pictures in question; he therefore never determined whether the sender was an adult. (Id., p. 37). In neither case did the Attorney General's office institute a prosecution. In fact, the Attorney General to date has not brought any prosecutions under the Act at all. (Id., p. 15). By contrast, Mr. McCartney described with justifiable pride his participation in the sting operation that resulted in the arrest of a student at SUNY who was using the Internet to contact a child; the defendant in that case, however, was charged under N.Y. Penal Law § 263, which prohibits an adult from promoting the sexual performance of a child. (Id., p. 12).

Balanced against the limited local benefits resulting from the Act is an extreme burden on interstate commerce. The New York Act casts its net worldwide; moreover, the chilling effect that it produces is bound to exceed the actual cases that are likely to be prosecuted, as Internet users will steer clear of the Act by significant margin. See ACLU, 929 F. Supp. at 863 (holding that individuals, uncertain of the reach of the CDA, will undoubtedly "'steer far wider of the unlawful zone'") (citing Bassett v. Bullitt, 377 U.S. 360, 372 (1964)); see also testimony of Maurice J. Freedman, Director of Westchester Library System, 4/7/97 Tr., at p. 209 ("My concern about prosecution in the context of this court proceeding is in relation to this Act. When I became aware of this Act and its implications for public libraries, as I perceived those implications, I at that point became quite concerned -- and scared might be another word -- for being arrested or being in violation."). At oral argument, the State asserted that only a small percentage of Internet communications are "harmful to minors" and would fall within the proscriptions of the statute; therefore, the State argued, the burden on interstate commerce is small. On the record before me, I conclude that the range of Internet communications potentially affected by the Act is far broader than the State suggests. I note that in the past, various communities within the United States have found works including I Know Why the Cared Bird Sings by Maya Angelou, Funhouse by Dean Koontz, The Adventures of Huckleberry Finn by Mark Twain, and The Color Purple by Alice Walker to be indecent. (Teicher Decl., p. 3). Even assuming, arguendo, that the Act applies only to pictures, a number of Internet users take advantage of the medium's capabilities to communicate images to one another and, again, I find that the range of images that might subject the communicator to prosecution (or reasonably cause a communicator to fear prosecution) is far broader than defendants assert. For example, many libraries, museums and academic institutions post art on the Internet that some might conclude was "harmful to minors." Famous nude works by Botticelli, Manet, Matisse, Cezanne and others can be found on the Internet. In this regard, I point out that a famous painting by Manet which shows a nude woman having lunch with two fully clothed men was the subject of considerable protest when it first was unveiled in Paris, as many observers believed that it was "scandalous." (Declaration of Judith F. Krug, sworn to in March, 1997, at p. 5). Lesser known artists who post work over the Internet may face an even greater risk of prosecution, because the mantle of respectability that has descended on Manet is not associated with their as yet obscure names. Lile Elam, the founder of Art on the Net, submitted a Declaration that included samples of the types of work found on Art on the Net's site; certain of the images might be considered harmful to minors in some communities, including several nudes and a very dark, disturbing short story entitled "Two Running Rails of Mercury," accompanied by a picture of a woman's nude body dissolving into railroad tracks. (Declaration of Lile Elam, sworn to on March 13, 1997, Exh. 6). Rudolf Kinsky testified to his perception of the greater risk run by an unrenowned artist who posts controversial images on the Internet; when he was asked by defendants if a work by Corbet could subject the artist to prosecution, he answered, "His works are established; they are known. This is a different situation. Could be or could not, but my situation, when I am at the beginning of my career, and someone can, because I am not known, I have no established name and everything, I can still be prosecuted." (4/7/97 Tr., at 250). Individuals who wish to communicate images that might fall within the Act's proscriptions must thus self-censor or risk prosecution, a Hobson's choice that imposes an unreasonable restriction

on interstate commerce. See Allen B. Dumont Labs., Inc. v. Carroll, 86 F. Supp. 813, 816 (1949) (holding that Pennsylvania state law requiring that motion pictures be submitted for review by a censorship board prior to being exhibited in the state imposed an undue and unreasonable burden on interstate commerce), aff'd, 184 F.2d 153 (3d Cir. 1950), cert. denied, 340 U.S. 929 (1951).

Moreover, as both three-judge panels that struck the federal statute have found, the costs associated with Internet users' attempts to comply with the terms of the defenses that the Act provides are excessive. Both courts that addressed the Communications Decency Act found that these costs of compliance, coupled with the threat of serious criminal sanctions for failure to comply, could drive some Internet users off the Internet altogether. See ACLU, 929 F. Supp. at 855-56 ("Many speakers who display arguably indecent content on the Internet must choose between silence and the risk of prosecution . . . [the] defenses are not technologically or economically feasible for most providers"); Shea, 930 F. Supp. at 942-48 (finding that the defenses provided by the CDA do not offer a safe harbor to Internet users, who are then faced with the choice between complying, despite economic and technological barriers, or refraining from the Internet posting that potentially subjects them to prosecution). While the defenses in the Act are not identical to those present in the CDA, the cost analysis undertaken by the ACLU and Shea courts is equally applicable to both statutes.

The severe burden on interstate commerce resulting from the New York statute is not justifiable in light of the attenuated local benefits arising from it. The alternative analysis of the Act as an indirect regulation on interstate commerce therefore also mandates the issuance of the preliminary injunction sought by plaintiffs.

D. The Act Unconstitutionally Subjects Interstate Use of the Internet to Inconsistent Regulations

Finally, a third mode of Commerce Clause analysis further confirms that the plaintiffs are likely to succeed on the merits of their claim that the New York Act is unconstitutional. The courts have long recognized that certain types of commerce demand consistent treatment and are therefore susceptible to regulation only on a national level. The Internet represents one of those areas; effective regulation will require national, and more likely global, cooperation. Regulation by any single state can only result in chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations. Without the limitations imposed by the Commerce Clause, these inconsistent regulatory schemes could paralyze the development of the Internet altogether.

In numerous cases, the Supreme Court has acknowledged the need for coordination in the regulation of certain areas of commerce. As long ago as 1886, the Supreme Court stated:

> Commerce with foreign countries and among the states, strictly considered, consists in intercourse and traffic, including in these terms navigation, and the transportation and transit of persons and property, as well as the purchase, sale, and exchange of commodities. For the regulation of commerce, as thus defined, there can be only one system of rules, applicable alike to the whole country; and the authority which can act for the whole country can alone adopt such a system. Action upon it by separate states is not, therefore, permissible.

Wabash, St. L. & P. Ry. Co. v. Illinois, 118 U.S. 557, 574-75 (1886). The Court in Wabash struck the Illinois statute at issue, which purported to establish interstate railway rates, stating "[t]hat this species of regulation is one which must be, if established at all, of a general and national character, and cannot be safely and wisely remitted to local rules and regulations, we think is clear from what has already been said." Id. at 577.

Similarly, in Southern Pac. Co. v. Arizona ex rel. Sullivan, 325 U.S. 761 (1945), the Court

addressed the constitutionality of an Arizona statute that limited the length of trains within the state to fourteen passenger and seventy freight cars. The lower court's findings demonstrated that 93% of the freight traffic and 95% of the passenger traffic in Arizona was interstate; moreover, the Court endorsed the findings that travel by trains of more than fourteen passenger cars and more than seventy freight cars over the main lines of the United States was standard practice, and that the Arizona law had the effect of forcing railroads to decouple their trains in Texas or New Mexico and reform the train at full length in California. Id. at 774. Thus, the practical impact of the Arizona law was to control the length of trains, as the Court put it, "all the way from Los Angeles to El Paso." Id. The Court concluded that the Arizona train limit law imposed a serious burden on interstate commerce, noting that various states had imposed varying limits. The Court stated:

> With such laws in force in states which are interspersed with those having no limit on train lengths, the confusion and difficulty with which interstate operations would be burdened under the varied system of state regulation and the unsatisfied need for uniformity in such regulation, if any, are evident.

Id. at 773-74. In striking the Arizona law as an unconstitutional intrusion on interstate commerce, the Court relied on a long-established rule barring the states from regulating "those phases of the national commerce which, because of the need of national uniformity, demand that their regulation, if any, be prescribed by a single authority." Id. at 766 (citing Gibbons v. Ogden, 9 Wheat. 1 (1824); Cooley v. Board of Wardens, 12 How. 299, 319 (1851); Leisy v. Hardin, 135 U.S. 100, 108-09 (1890); Minnesota Rate Cases, 230 U.S. 399, 400 (1913); Edwards v. People of State of California, 314 U.S. 160, 176 (1941)).

In Bibb v. Navajo Freight Lines, Inc., 359 U.S. 520 (1959), the Court examined an Illinois statute that required the use of contour mudguards on trucks in Illinois. The Court took note of the fact that straight or conventional mudguards were permissible in most other states and actually required in Arkansas. Id. at 526. Recognizing the need for coordinated legislation, the Court stated that "[t]he conflict between the Arkansas regulation and the Illinois regulation . . . suggests that this regulation of mudguards is not one of those matters 'admitting of diversity of treatment, according to the special requirements of local conditions.'" Id. at 528 (quoting Sproles v. Binford, 286 U.S. 374, 390 (1932)). The Court struck the Illinois law as imposing an undue burden on interstate commerce, in part because Illinois was insisting upon "a design out of line with the requirements of almost all the other states." Id.

The Internet, like the rail and highway traffic at issue in the cited cases, requires a cohesive national scheme of regulation so that users are reasonably able to determine their obligations. Regulation on a local level, by contrast, will leave users lost in a welter of inconsistent laws, imposed by different states with different priorities. New York is not the only state to enact a law purporting to regulate the content of communications on the Internet. Already Oklahoma and Georgia have enacted laws designed to protect minors from indecent communications over the Internet; as might be expected, the states have selected different methods to accomplish their aims. Georgia has made it a crime to communicate anonymously over the Internet, while Oklahoma, like New York, has prohibited the online transmiaaion of material deemed harmful to minors. See Ga. Code Ann. § 16-19-93.1 (1996); Okla. Stat. tit. 21, § 1040.76 (1996).

Moreover, the regulation of communications that may be "harmful to minors" taking place over the Internet poses particular difficulties. New York has defined "harmful to minors" as including:

> that quality of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse, when it:
> (a) Considered as a whole, appeals to the prurient interest in sex of minors; and
> (b) Is patently offensive to prevailing standards in the adult community as a

> whole with respect to what is suitable material for minors; and
> (c) Considered as a whole, lacks serious literary, artistic, political and scientific value for minors.

N.Y. Penal Law § 235.20(6). Courts have long recognized, however, that there is no single "prevailing community standard" in the United States. Thus, even were all 50 states to enact laws that were verbatim copies of the New' York Act, Internet users would still be subject to discordant responsibilities. To use an example cited by the court in ACLU v. Reno, the Broadway play Angels in America, which concerns homosexuality and AIDS and features graphic language, was immensely popular in New York and in fact earned two Tony awards and a Pulitzer prize. ACLU, 929 F. Supp. at 852-53. In Charlotte, North Carolina, however, a production of the drama caused such a public outcry that the Mecklenberg County Commission voted to withhold all public funding from arts organizations whose works "expose the public to perverted forms of sexuality." Eric Harrison, Charlotte Ban on Funding Questions Community Culture Commission -- Boycotts "Perverted Sexuality", Milwaukee J. & Sentinel, April 21, 1997, at 3. The Supreme Court has always recognized that "our nation is simply too big and too diverse for this Court to reasonably expect that such standards [of what is patently offensive] could be articulated for all 50 states in a single formulation." Miller, 413 U.S. at 30.

As discussed at length above, an Internet user cannot foreclose access to her work from certain states or send differing versions of her communication to different jurisdictions. In this sense, the Internet user is in a worse position than the truck driver or train engineer who can steer around Illinois or Arizona, or change the mudguard or train configuration at the state line; the Internet user has no ability to bypass any particular state. The user must thus comply with the regulation imposed by the state with the most stringent standard or forego Internet communication of the message that might or might not subject her to prosecution. For example, a teacher might invite discussion of Angels In America from a Usenet newsgroup dedicated to the literary interests of high school students. Quotations from the play might not subject her to prosecution in New York[10] -- but could qualify as "harmful to minors.-s" according to the community standards prevailing in Oklahoma. The teacher cannot tailor her message on a community specific basis and thus must take her chances or avoid the discussion altogether.

Further development of the Internet requires that users be able to predict the results of their Internet use with some degree of assurance. Haphazard and uncoordinated state regulation can only frustrate the growth of cyberspace. The need for uniformity in this unique sphere of commerce requires that New York's law be stricken as a violation of the Commerce Clause.

III. The First Amendment and the Internet

Plaintiffs have also asserted their entitlement to a preliminary injunction on the grounds that the Act unconstitutionally burdens free speech. Plaintiffs' ready ability to demonstrate the Act's unconstitutionality under the Commerce Clause, however, provides fully adequate support for the issuance of a preliminary injunction at this time. Moreover, the Supreme Court heard argument on a First Amendment challenge to the federal statute, the CDA, on March 19, 1997. The State vigorously argues that its law was designed to avoid the constitutional pitfalls presented by the CDA; however, the New York Act was clearly modelled on the CDA, and numerous provisions of the New York Act mirror their federal counterparts. See New York State Executive Charter Memorandum, annexed as Exhibit A to Declaration of Anat Hakim, sworn to on March 21, 1997 ("This bill . . . is consistent with the federal statute"); Letter from William Sears to Governor Pataki, dated July 11, 1996, annexed as Exhibit A to Hershler Aff't ("This bill is consistent with the Federal Communications Decency Act"); Introducer's Memorandum in Support of Amended Senate Bill S. 210-E and Assembly Bill A. 3967-C, annexed as Exhibit G to Hershler Aff't ("'Amendments were necessary-for the bill to be consistent with the recently passed Federal

Communications Decency Act . . . . Furthermore, it should be noted that the 'harmful to minors' standard contained in the charging language of the offense is consistent with the Federal law . . . ."). I believe any determination of plaintiffs' First Amendment challenge should therefore await the guidance to be provided by the Supreme Court's forthcoming opinion.

CONCLUSION

The protection of children from pedophilia is an entirely valid and laudable goal of state legislation. The New York Act's attempts to effectuate that goal, however, fall afoul of the Commerce Clause for three reasons. First, the practical impact of the New York Act results in the extraterritorial application of New York law to transactions involving citizens of other states and is therefore per se violative of the Commerce Clause. Second, the benefits derived from the Act are inconsequential in relation to the severe burdens it imposes on interstate commerce. Finally, the unique nature of cyberspace necessitates uniform national treatment and bars the states from enacting inconsistent regulatory schemes. Because plaintiffs have demonstrated that they are likely to succeed on the merits of their claim under the Commerce Clause and that they face irreparable injury in the absence of an injunction, the motion for a preliminary injunction is granted.

Defendants are enjoined from instituting any prosecutions under the Act, until further Order of this Court. Plaintiffs shall submit a proposed form of injunction on two days' notice.

SO ORDERED:

Dated: New York, New York, June 20, 1997

LORETTA A. PRESKA, U.S.D.J.

NOTES

1. I recall in this respect a particularly confusing item of testimony elicited at the evidentiary hearing. Ms. Kovacs, plaintiffs' expert witness with respect to the Internet, testified that on one occasion while she was in a MUD (a Multi User Dungeon), a malefactor sicced his "virtual dog" on her because she had trespassed on his domain. Fortunately, the other inhabitants of the MUD came to her rescue, vehemently protesting the unfriendliness of the virtual canine attack. Relieved as I was that the story had a happy ending, I must admit that it afforded me a window into an entirely unknown world. (4/4/97 Tr., p. 95).

2. Where information in this subsection is not cited to ACLU or Shea, it was derived from the parties' Joint Stipulation of Facts.

3. Because I find, as discussed below, that plaintiffs have demonstrated a likelihood of success on the merits of their claim that the New York Act violates the Commerce Clause, I do not rely on the "fair ground for litigation" standard. I note, however, that the standard would be applicable to this case because: (1) the action alleges constitutional violations, Almonte v. Pierce, 666 F. Supp. 517, 526 (S.D.N.Y. 1987); (2) the public interest in a free flow of interstate commerce served by an injunction against enforcement of the Act counterbalances the public interest in protecting children served by the Act, see Carey v. Klutznick, 637 F.2d 834, 839 (2d Cir. 1980); and (3) the New York Legislature did not engage in any fact-finding regarding the public interest served by the Act before promulgating it. Able v. United States, 44 F.3d 128, 131 (2d Cir. 1995).

4. Other jurisdictions internationally have also gotten into the act. In January, 1997, two associations dedicated to the preservation of France's linguistic purity filed suit against two

private corporations and Georgia Tech Lorraine, a French university affiliated with the Georgia Institute of Technology, claiming that the defendants violated a French law that prohibits advertising in any language other than French by operating English-language sites on the World Wide Web. See Complaint filed by L' Association "Avenir de la Lengue Francaise" and L'Association "Defense de La Lengue Francaise," Jan. 6, 1996; see also E. Schneiderman & R. Kornreich, Personal Jurisdiction and Internet Commerce, N.Y.L.J., June 4, 1997, at 1. The French court dismissed the action as to Georgia Tech, but other efforts by foreign jurisdictions to regulate the Internet are likely to follow. In addition, Germany made headlines recently when its anti-pornography laws forced Compuserve to close access to over 200 Internet sites from anywhere in the world. See John Markoff, Compuserve Bars Access to Internet Sex: German Laws Prompt the Provider to Block Pictures and Chat Groups, Orange County Register, December 29, 1995.

5. The defendants proposed Ms. Pirro as a witness for the evidentiary hearing, but then withdrew the proposal. Ms. Pirro's letter, which preceded the bill's signature into law by the Governor, is properly considered as part of the legislative history. See Civil Service Employees Association. Inc. v. Oneida, 78 A.D.2d 1004, 1005 (4th Dep't 1980), appeal denied, 53 N.Y.2d 603 (1981). Ms. Pirro's testimony, on the other hand, would be a hindsight, post-enactment review of legislative intent by a non-legislator and would carry no probative weight. See Bread Political Action Committee v. Federal Election Committee, 455 U.S. 577, 580 n.3 (1982); Frontier Ins. Co. v. New York, 609 N.Y.S.2d 748, 752 (N.Y. Ct. Cl. 1993), aff'd, 197 A.D.2d 177 (3d Dep't 1994).

6. Judge Stein recently concluded that these realities meant that one whose only contact with the forum occurs via the Internet is not susceptible to suit there. Bensusan Restaurant Corp. v. King, 937 F. Supp. 295 (S.D.N.Y. 1996).

7. The Court's injunction against extraterritorial regulation is long-established. See Huntington v. Attrill, 146 U.S. 657, 669 (1892) ("Laws have no force of themselves beyond the jurisdiction of the State which enacts them, and can have extraterritorial effect only by the comity of other States); New York Life Ins. Co. v. Head, 234 U.S. 149, 161 (1914) ("[I]t would be impossible to permit the statutes of Missouri to operate beyond the jurisdiction of that State . . . without throwing down the constitutional barriers by which all the States are restricted within the orbits of their lawful authority and upon the preservation of which the Government under the Constitution depends. This is so obviously the necessary result of the Constitution that it has rarely been called in question and hence authorities dealing directly with it do not abound.").

8. The distinction between direct regulations of interstate commerce, which are subject to a per se rule of invalidation, and indirect regulations subject to the less stringent balancing test has never been sharply defined. In either situation, however, the "critical consideration is the overall effect of the statute on both local and interstate activity." See Brown-Forman, 476 U.S. at 579; Raymond Motor Transportation. Inc. v. Rice, 434 U.S. 429, 440-41 (1978).

9. The state's construction of the Act is unsupportable in light of the plain language of the statute and the interpretation that has been applied to closely related statutes. The Act applies to "communication[s] which, in whole or in part, depict[] actual or simulated nudity, sexual conduct or sado-masochistic abuse, and which [are] harmful to minors." The defendants contend that "depict" embraces only pictorial images. The dictionary definition of "depict," however, includes both visual representations and "description." Webster's Third New International Dictionary 605 (1981). The Act itself defines material that is harmful to minors as including any "description or representation," supporting an interpretation of the word "depict" that includes both text and pictures. Further, the Act is intended to extend liability under the statute as it existed prior to amendment. Cases brought under the prior law confirmed its applicability to sexually frank text, as well as pictures. See People v. Lida, 247 N.Y.S.2d 421 (N.Y. City Crim. Ct.) (finding that magazine containing short stories dealing with sex as well as photographs showing nude and partially nude

women fell within the prohibition of Penal Law 1909 § 484-h [now Penal Law § 235.21], proscribing sale of magazines to minors), aff'd, 252 N.Y.S.2d 142 (N.Y. Sup. 1964); see also People v. Ginsberg, 290 N.Y.S.2d 239 (N.Y. Dist. 1966) (holding that evidence demonstrating that defendant, knowing buyer to be under 17, sold material containing pictures and photographs depicting female nudity and verbal descriptions and narrative accounts of sexual conduct and excitement was sufficient to sustain conviction for selling material harmful to minors), aff'd, 390 U.S. 619 (1968).

10. Further distinctions may exist within the state of New York. The community standards prevailing in New York City may well be different than the community standards prevailing in, for example, Rensselaer County. See. e.g., United States v. Various Articles of Obscene Merchandise Schedule No. 2102, 709 F.2d 132, 134, 137 (2d Cir. 1983) (upholding the district court's conclusion that "detailed portrayals of genitalia, sexual intercourse, fellatio, and masturbation" including the film "Deep Throat" and other pornographic films and magazines, are not obscene, "in light of the community standards prevailing in New York City.")

INDEX | JOIN | HOME | SEARCH | FEEDBACK

Copyright 1997, The American Civil Liberties Union

LAW JOURNAL EXTRA! HOME

Why Surf

TABLE OF CONTENTS | MARKETPLACE | NEWS | EMPLOYMENT | PRACTICE AREAS | RESOURCES | LAW/TECH | LAW FIRMS

NEW YORK LAW JOURNAL

Decision of the Day: Brower v. Gateway 2000

New York Law Journal
August 17, 1998

Brower, et. al.,

plaintiffs-appellants;

Levy, et al., plaintiffs,

v. Gateway 2000, Inc., et al.,

defendants-respondents.

Before Milonas, J.P.; Nardelli, *Mazzarelli and Saxe, JJ.*

QDS:12102050

PLAINTIFFS appeal from an order of the Supreme Court, New York County (Beatrice Shainswit, J.), entered Oct. 21, 1997, which, to the extent appealed from, granted defendants' motion to dismiss the complaint on the ground that there was a valid agreement to arbitrate between the parties.

Thomas A. Holman, of counsel (Zachary Alan Starr, on the brief, Starr & Holman, attorneys) for plaintiffs-appellants,

Robert M. Rader, of counsel (Daniel R. Murdock and Alan B. Howard, on the brief, Winston & Strawn, attorneys) for defendants-respondents.

MILONAS, J.P. -- Appellants are among the many consumers who purchased computers and software products from defendant Gateway 2000 through a direct-sales system, by mail or telephone order. As of July 3, 1995, it was Gateway's practice to include with the materials shipped to the purchaser along with the merchandise a copy of its "Standard Terms and Conditions Agreement" and any relevant warranties for the products in the shipment. The Agreement begins with a "NOTE TO CUSTOMER," which provides, in slightly larger print than the remainder of the document, in a box that spans the width of the page: "This document contains Gateway 2000's Standard Terms and Conditions. By keeping your Gateway 2000 computer system beyond thirty (30) days after the date of delivery, you accept these Terms and Conditions." The document consists of 16 paragraphs, and, as is relevant to this appeal, paragraph 10 of the

agreement, entitled "DISPUTE RESOLUTION," reads as follows:

> Any dispute or controversy arising out of or relating to this Agreement or its interpretation shall be settled exclusively and finally by arbitration. The arbitration shall be conducted in accordance with the Rules of Conciliation and Arbitration of the International Chamber of Commerce. The arbitration shall be conducted in Chicago, Illinois, U.S.A. before a sole arbitrator. Any award rendered in any such arbitration proceeding shall be final and binding

on each of the parties, and judgment may be entered thereon in a court of competent jurisdiction.

Plaintiffs commenced this action on behalf of themselves and others similarly situated for compensatory and punitive damages, alleging deceptive sales practices in seven causes of action, including breach of warranty, breach of contract, fraud and unfair trade practices. In particular, the allegations focused on Gateway's representations and advertising

that promised "service when you need it," including around-the-clock free technical support, free software technical support and certain on-site services. According to plaintiffs, not only were they unable to avail themselves of this offer because it was virtually impossible to get through to a technician, but also Gateway continued to advertise this claim notwithstanding numerous complaints and reports about the problem.

Insofar as is relevant to appellants, who purchased their computers after July 3, 1995, Gateway moved to dismiss the complaint based on the arbitration clause in the Agreement. Appellants argued that the arbitration clause is invalid under UCC 2-207, unconscionable under UCC 2-302 and an unenforceable contract of adhesion. Specifically, they claimed that the provision was obscure; that a customer could not reasonably be expected to appreciate or investigate its meaning and effect; that the International Chamber of Commerce ("ICC") was not a forum commonly used for consumer matters; and that because ICC headquarters were in France, it was particularly difficult to locate the organization and its rules. To illustrate just how inaccessible the forum was, appellants advised the court that the ICC was not registered with the Secretary of State, that efforts to locate and contact the ICC had been unsuccessful and that apparently the only way to attempt to contact the ICC was through the United States Council for International Business, with which the ICC maintained some sort of relationship.

In support of their arguments, appellants submitted a copy of the ICC's Rules of Conciliation and Arbitration and contended that the cost of ICC arbitration was prohibitive, particularly given the amount of the typical consumer claim involved. For example, a claim of less than $50,000 required advance fees of $4,000 (more than the cost of most Gateway products), of which the $2000 registration fee was nonrefundable even if the consumer prevailed at the arbitration. Consumers would also incur travel expenses disproportionate to the damages sought, which appellants' counsel estimated would not exceed $1,000 per customer in this action, as well as bear the cost of Gateway's legal fees if the consumer did not prevail at the arbitration; in this respect, the ICC rules follow the "loser pays" rule used in England. Also, although Chicago was designated as the site of the actual arbitration, all correspondence must be sent to ICC headquarters in France.

The IAS court dismissed the complaint as to appellants based on the arbitration clause in the Agreements delivered with their computers. We agree with the court's decision and reasoning in all respects but for the issue of the unconscionability of the designation of the ICC as the arbitration body.

2-207

First, the court properly rejected appellants' argument that the arbitration clause was invalid under UCC 2-207. Appellants claim that when they placed their order they did not bargain for, much less accept, arbitration of any dispute, and therefore the arbitration clause in the agreement that accompanied the merchandise shipment was a "material alteration" of a pre-existing oral agreement. Under UCC 2-207(2), such a material alteration constitutes "proposals for addition to the contract" that become part of the contract only upon appellants' express acceptance. However, as the court correctly concluded, the clause was not a "material alteration" of an oral agreement, but, rather, simply one provision of the sole contract that existed between the parties. That contract, the court explained, was formed and acceptance was manifested not when the order was placed but only with the retention of the merchandise beyond the 30 days specified in the Agreement enclosed in the shipment of merchandise. Accordingly, the contract was outside the scope of UCC 2-207.

In reaching its conclusion, the IAS court took note of the litigation in Federal courts on this very issue, and, indeed, on this very arbitration clause. In *Hill v. Gateway 2000, Inc.* (105 F3d 1147, *cert denied* __US__, 118 S Ct 47), plaintiffs in a class action contested the identical Gateway contract in dispute before us, including the enforceability of the arbitration clause. As that court framed the issue,

the "[t]erms inside Gateway's box stand or fall together. If they constitute the parties contract because the Hills had an opportunity to return the computer after reading them, then all must be enforced" (*id.* at 1148). The court then concluded that the contract was not formed with the placement of a telephone order or with the delivery of the goods. Instead, an enforceable contract was formed only with the consumer's decision to retain the merchandise beyond the 30-day period specified in the agreement. Thus, the agreement as a whole, including the arbitration clause, was enforceable.

This conclusion was in keeping with the same court's decision in *ProCD, Inc. v. Zeidenberg* (86 F3d 1447), where it found that detailed terms enclosed within the packaging of particular computer software purchased in a retail outlet constituted the contract between the vendor and the consumer who retained the product. In that case, the Seventh Circuit held that UCC 2-207 did not apply and indeed was "irrelevant" to such transactions, noting that the section is generally invoked where multiple agreements have been exchanged between the parties in a classic "battle of the forms," whereas *ProCD* (as well as *Hill* and this case) involves but a single form (*id.* at 1452).

The *Hill* decision, in its examination of the formation of the contract, takes note of the realities of conducting business in today's world. Transactions involving "cash now, terms later" have become commonplace, enabling the consumer to make purchases of sophisticated merchandise such as computers over the phone or by mail -- and even by computer. Indeed, the concept of "[p]ayment preceding the revelation of full terms" is particularly common in certain industries, such as air transportation and insurance (*id.* at 1149; *ProCD v. Zeidenberg*, *supra*, at 1451).

While *Hill* and *ProCD*, as the IAS court recognized, are not controlling (although they are decisions of the United States Court of Appeals for the circuit encompassing the forum state designated for arbitration), we agree with their rationale that, in such transactions, there is no agreement or contract upon the placement of the order or even upon the receipt of the goods. By the terms of the Agreement at issue, it is only after the consumer has affirmatively retained the merchandise for more than 30 days -- within which the consumer has presumably examined and even used the product(s) and read the agreement -- that the contract has been effectuated. In this respect, the case is distinguishable from *S&T Sportswear v. Drake Fabrics* (190 AD2d 598), cited by appellants, where this Court found that an arbitration clause found on the reverse side of defendant's draft sales contract did constitute a "material alteration" where the parties did in fact have a pre-existing oral agreement.

While appellants argue that *Hill* is contrary to the law of New York in that it departs from the holding of cases such as *Matter of Marlene v. Carnac Textiles* (45 NY2d 327) and its progeny, we disagree with their interpretation of both cases: *Hill* not only involves one form only, as distinguished from the "battle of the forms" scenario of the cases appellants cite, but these cases are simply inapplicable because, as explained, no contract was formed here or in *Hill* until the merchandise was retained beyond the 30-day period. The disputed arbitration clause is simply one provision of the sole contract "proposed" between the parties.

C.O.A.

Second, with respect to appellants' claim that the arbitration clause is unenforceable as a contract of adhesion, in that it involved no choice or negotiation on the part of the consumer but was a "take it or leave it" proposition (*see, e.g., Matter of State v. Ford Motor Company*, 74 NY2d 495, 503), we find that this argument, too, was properly rejected by the IAS court. Although the parties clearly do not possess equal bargaining power, this factor alone does not invalidate the contract as one of adhesion. As the IAS court observed, with the ability to make the purchase elsewhere and the express option to return the goods, the consumer is not in a "take it or leave it" position at all; if any term of the agreement is unacceptable to the consumer, he or she can easily buy a competitor's product instead -- either from a retailer or directly from the manufacturer -- and reject Gateway's agreement by returning the merchandise (*see, e.g., Carnival Cruise Lines v. Shute*, 499 US 585, 593-594; *Fidelity and Deposit Company of Maryland v. Altman*, 209 AD2d 195, *lv denied* 91 NY2d 805). The consumer has 30 days to make that decision. Within that time, the consumer can inspect the goods and examine and seek clarification of the terms of the agreement; until those 30 days have elapsed, the consumer has the unqualified right to return the merchandise, because the goods or terms are unsatisfactory or for no reason at all.

~~While returning the goods to avoid the formation of the contract entails affirmative action on the~~

While returning the goods to avoid the formation of the contract entails affirmative action on the part of the consumer, and even some expense, this may be seen as a trade-off for the convenience and savings for which the consumer presumably opted when he or she chose to make a purchase of such consequence by phone or mail as an alternative to on-site retail shopping. That a consumer does not read the agreement or thereafter claims he or she failed to understand or appreciate some term therein does not invalidate the contract any more than such claim would undo a contract formed under other circumstances (*see, e.g., Morris v. Snappy Car Rental, Inc.*, 84 NY2d 21, 30). We further note that appellants' claim of adhesion is identical to that made and rejected in *Filias v. Gateway 2000, Inc.*, an unreported case brought to our attention by both parties that interprets the same Gateway agreement (No. 97C 2523 [N.D. Ill., January 15, 1998, *transferred by* 1997 US Dist LEXIS 7115 [E.D. Mich]).

Unconscionable Finally, we turn to appellants' argument that the IAS court should have declared the contract unenforceable, pursuant to UCC 2-302, on the ground that the arbitration clause is unconscionable due to the unduly burdensome procedure and cost for the individual consumer. The IAS court found that while a class-action lawsuit, such as the one herein, may be a less costly alternative to the arbitration (which is generally less costly than litigation), that does not alter the binding effect of the valid arbitration clause contained in the agreement (*see, Harris v. Shearson Hayden Stone*, 82 AD2d 87, 92-93, *affd* 56 NY2d 627 *for reasons stated below*; *see also, Matter of Ball*, 236 AD2d 158, *appeal dismissed* 91 NY2d 921).

As a general matter, under New York law, unconscionability requires a showing that a contract is "both procedurally and substantively unconscionable when made" (*Gillman v. Chase Manhattan Bank*, 73 NY2d 1, 10). That is, there must be "some showing of 'an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favorable to the other party' [citation omitted]" (*Matter of State of New York v. Avco Financial Services*, 50 NY2d 383, 389-390). The *Avco* court took pains to note, however, that the purpose of this doctrine is not to redress the inequality between the parties but simply to ensure that the more powerful party cannot "surprise" the other party with some overly oppressive term (*id.*).

As to the procedural element, a court will look to the contract formation process to determine if in fact one party lacked any meaningful choice in entering into the contract, taking into consideration such factors as the setting of the transaction, the experience and education of the party claiming unconscionability, whether the contract contained "fine print," whether the seller used "high-pressured tactics" and any disparity in the parties' bargaining power (*Gillman v. Chase Manhattan Bank, supra*, at 10-11). None of these factors supports appellants' claim here. Any purchaser has 30 days within which to thoroughly examine the contents of their shipment, including the terms of the Agreement, and seek clarification of any term therein (*e.g., Matter of Ball, supra*, at 161). The Agreement itself, which is entitled in large print "STANDARD TERMS AND CONDITIONS AGREEMENT," consists of only three pages and 16 paragraphs, all of which appear in the same size print. Moreover, despite appellants' claims to the contrary, the arbitration clause is in no way "hidden" or "tucked away" within a complex document of inordinate length, nor is the option of returning the merchandise, to avoid the contract, somehow a "precarious" one. We also reject appellants' insinuation that, by using the word "standard," Gateway deliberately meant to convey to the consumer that the terms were standard within the industry, when the document clearly purports to be no more than *Gateway's* "standard terms and conditions."

With respect to the substantive element, which entails an examination of the substance of the agreement in order to determine whether the terms unreasonably favor one party (*Gillman v. Chase Manhattan Bank, supra*, 73 NY2d, at 12), we do not find that the possible inconvenience of the chosen site (Chicago) alone rises to the level of unconscionability. We do find, however, that the excessive cost factor that is necessarily entailed in arbitrating before the ICC is unreasonable and surely serves to deter the individual consumer from invoking the process (*see, Matter of Teleserve Systems*, 230 AD2d 585, 594, *lv denied* __NY2d__, 1997 NY App Div LEXIS 10626). Barred from resorting to the courts by the arbitration clause in the first instance, the designation of a financially prohibitive forum effectively bars consumers from this forum as well; consumers are thus left with no forum at all in which to resolve a dispute. In this regard, we note that this particular claim is not mentioned in the *Hill* decision, which upheld the clause as part of an enforceable contract.

While it is true that, under New York law, unconscionability is generally predicated on the

presence of both the procedural and substantive elements, the substantive element alone may be sufficient to render the terms of the provision at issue unenforceable (*see*, *Gillman v. Chase Manhattan Bank*, *supra*, at 12; *Matter of State of New York v. Avco Financial Services*, *supra*, at 389; *State of New York v. Wolowitz*, 96 AD2d 47, 68). Excessive fees, such as those incurred under the ICC procedure, have been grounds for finding an arbitration provision unenforceable or commercially unreasonable (*see*, *e.g.*, *Matter of Teleserve Systems*, *supra*, at 593-594).

In the *Filias* case previously mentioned, the Federal District Court stated that it was "inclined to agree" with the argument that selection of the ICC rendered the clause unconscionable, but concluded that the issue was moot because Gateway had agreed to arbitrate before the American Arbitration Association ("AAA") and sought court appointment of the AAA pursuant to Federal Arbitration Act 9 USC §5. The court accordingly granted Gateway's motion to compel arbitration and appointed the AAA in lieu of the ICC. Plaintiffs in that action (who are represented by counsel for appellants before us) contend that costs associated with the AAA process are also excessive, given the amount of the individual consumer's damages, and their motion for reconsideration of the court's decision has not yet been decided. While the AAA rules and costs are not part of the record before us, the parties agree that there is a minimum, nonrefundable filing fee of $500, and appellants claim each consumer could spend in excess of $1,000 to arbitrate in this forum.

Gateway's agreement to the substitution of the AAA is not limited to the *Filias* plaintiffs. Gateway's brief includes the text of a new arbitration agreement that it claims has been extended to all customers, past, present and future (apparently through publication in a quarterly magazine sent to anyone who has ever purchased a Gateway product). The new arbitration agreement provides for the consumer's choice of the AAA or the ICC as the arbitral body and the designation of any location for the arbitration by agreement of the parties, which "shall not be unreasonably withheld." It also provides telephone numbers at which the AAA and the ICC may be reached for information regarding the "organizations and their procedures."

As noted, however, appellants complain that the AAA fees are also excessive and thus in no way have they accepted defendant's offer (*see*, UCC 2-209); because they make the same claim as to the AAA as they did with respect to the ICC, the issue of unconscionability is not rendered moot, as defendant suggests. We cannot determine on this record whether the AAA process and costs would be so "egregiously oppressive" that they, too, would be unconscionable (*Avildsen v. Prystay*, 171 AD2d 13, 14, *appeal dismissed*, 79 NY2d 841). Thus, we modify the order on appeal to the extent of finding that portion of the arbitration provision requiring arbitration before the ICC to be unconscionable and remand to Supreme Court so that the parties have the opportunity to seek appropriate substitution of an arbitrator pursuant to the Federal Arbitration Act (9 USC §1 et seq.), which provides for such court designation of an arbitrator upon application of either party, where, for whatever reason, one is not otherwise designated (9 USC §5).

Appellants make the final argument that the arbitration clause does not apply to the cause of action for false advertising (with respect to the promised round-the-clock service) under various sections of the General Business Law on the ground that there is no mention of arbitration in the technical service contract itself. Although they raise this claim for the first time on this appeal, we find the promise of technical support to be within the scope of arbitration as it is clearly a "dispute or controversy arising out or relating to [the] Agreement or its interpretation." Put another way, the service contract does not apply to some separate product that could be retained while the computer products -- and the accompanying agreement -- could be returned.

Accordingly, the order of Supreme Court, New York County (Beatrice Shainswit, J.), entered Oct. 21, 1997, which, to the extent appealed from, granted defendants' motion to dismiss the complaint as to appellants on the ground that there was a valid agreement to arbitrate between the parties, should be modified, on the law and the facts, to the extent of vacating that portion of the arbitration agreement as requires arbitration before the International Chamber of Commerce, with leave to the parties to seek appointment of an arbitrator pursuant to 9 USC § 5 and remanding the matter for that purpose, and otherwise affirmed, without costs.

California Assembly Bill 1629

AB 1629

Introduced by Assembly Member Gary G. Miller, January 5, 1998
As passed by Senate on August 26, 1998
(Assembly concurred in Senate amendments on August 27, 1998)

An act to amend Section 17511.1 of, and to add Section 17538.45 to, the Business and Professions Code, and to amend Section 502 of the Penal Code, relating to advertising.

LEGISLATIVE COUNSEL'S DIGEST

AB 1629, as amended, Miller. Advertising: telephonic sellers: electronic mail.

(1) Existing law provides for the regulation of telephonic sellers, as defined. It exempts from the definition of telephonic sellers certain specified persons.

This bill would add to those persons exempt from the definition of telephonic sellers certain nonprofit corporations that have been exempt from taxation under a specified provision of the Revenue and Taxation Code for a minimum of 10 years, that have maintained their principal purpose for a minimum of 10 years, and that have been incorporated in the state for a minimum of 25 years.

(2) Existing law prohibits a person conducting business in this state from faxing unsolicited advertising material, unless certain conditions are satisfied.

This bill would also prohibit a registered user of an electronic mail service provider, as defined, from using or causing to be used the provider's equipment located in this state in violation of the provider's policy prohibiting or restricting the use of its equipment for the initiation of unsolicited electronic mail advertisements. It would also prohibit any individual, corporation, or other entity from using or causing to be used, by initiating an unsolicited electronic mail advertisement, an electronic mail service provider's equipment located in this state in violation of the provider's policy prohibiting or restricting the use of its equipment to deliver unsolicited electronic mail advertisements to its registered users. It would authorize any electronic mail service provider whose policy is violated as provided in these provisions to bring, in addition to any other action available under law, a civil action to recover damages, as specified, and would authorize the court to award reasonable attorney's fees to a prevailing party in that action.

(3) Existing law makes it a crime to knowingly and without permission tamper with, interfere with, damage, or gain unlawful access to certain computers, computer systems, and computer data.

This bill would, in addition, make it a crime to knowingly and without permission use the Internet domain name, as defined, of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damage or cause damage to a computer, computer system, or computer network. By creating a new crime, this bill would impose a state-mandated local program.

(4) The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: yes.

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

~~**SECTION 1.** Section 17511.1 of the Business and Professions Code is amended to read:~~

17511.1 As used in this article, "telephonic seller" or "seller" means a person who, on ~~his or her own behalf or through salespersons or through the use of an automatic~~

Dealers, Inc., if the exchange or interdealer quotation system has been certified by rule or order of the Commissioner of Corporations under subdivision (o) of Section 25100 of the Corporations Code. A subsidiary of an issuer that qualifies for exemption under this paragraph is not itself exempt unless not less than 60 percent of the voting power of its shares is owned by the qualifying issuer or issuers.

(17) A person soliciting exclusively the sale of telephone answering services to be provided by that person or that person's employer.

(18) A person soliciting a transaction regulated by the Commodity Futures Trading Commission if the person is registered or temporarily licensed for this activity with the Commodity Futures Trading Commission under the Commodity Exchange Act, (7 U.S.C. Sec. 1 et seq.), and the registration or license has not expired or been suspended or revoked.

(19) A person who sells coins or bullion at a price which is not more than 25 percent more than the price at which the seller is concurrently buying the same coins or bullion, if: (A) the seller has had a retail location in California from which he or she has been selling coins or bullion to the public in person for at least three years; (B) the telephonic solicitations are not the person's primary business and sales made telephonically make up less than 20 percent of the person's total retail sales; and (C) the person claiming an exemption pursuant to this subdivision complies with Section 17511.3, as applicable, and subdivision (p) of Section 17511.4.

(20) A person licensed pursuant to Chapter 14 (commencing with Section 1800) of Division 1 of the Financial Code to receive money for transmittal to foreign countries if the license has not expired or been suspended or revoked.

(21) A person licensed as a residential mortgage lender or servicer pursuant to Division 20 (commencing with Section 50000) of the Financial Code, when acting under the authority of that license.

(22) A corporation that meets all of the following conditions:

(A) It has been exempt from taxation under Section 23701e of the Revenue and Taxation Code for a minimum of 10 years.

(B) It has maintained its principal purpose for a minimum of 10 years.

(C) It has been incorporated in the state for a minimum of 25 years.

(f) In any civil proceeding alleging a violation of this article, the burden of proving an exemption or an exception from a definition is upon the person claiming it, and in any criminal proceeding alleging a violation of this article, the burden of producing evidence to support a defense based upon an exemption or an exception from a definition is upon the person claiming it.

(g) Compliance with this article does not satisfy nor substitute for any requirements for license, registration, or regulation mandated by other laws.

SEC. 2. Section 17538.45 is added to the Business and Professions Code, to read:

17538.45. (a) For purposes of this section, the following words have the following

meanings:

(1) "Electronic mail advertisement" means any electronic mail message, the principal purpose of which is to promote, directly or indirectly, the sale or other distribution of goods or services to the recipient.

(2) "Unsolicited electronic mail advertisement" means any electronic mail advertisement that meets both of the following requirements:

(A) It is addressed to a recipient with whom the initiator does not have an existing business or personal relationship.

(B) It is not sent at the request of or with the express consent of the recipient.

(3) "Electronic mail service provider" means any business or organization qualified to do business in California that provides registered users the ability to send or receive electronic mail through equipment located in this state and that is an intermediary in sending or receiving electronic mail.

(4) "Initiation" of an unsolicited electronic mail advertisement refers to the action by the initial sender of the electronic mail advertisement. It does not refer to the actions of any intervening electronic mail service provider that may handle or retransmit the electronic message.

ISP safe harbor?

(5) "Registered user" means any individual, corporation, or other entity that maintains an electronic mail address with an electronic mail service provider.

(b) No registered user of an electronic mail service provider shall use or cause to be used that electronic mail service provider's equipment located in this state in violation of that electronic mail service provider's policy prohibiting or restricting the use of its service or equipment for the initiation of unsolicited electronic mail advertisements.

Restriction on registered user

(c) No individual, corporation, or other entity shall use or cause to be used, by initiating an unsolicited electronic mail advertisement, an electronic mail service provider's equipment located in this state in violation of that electronic mail service provider's policy prohibiting or restricting the use of its equipment to deliver unsolicited electronic mail advertisements to its registered users.

protection of CA servers

(d) An electronic mail service provider shall not be required to create a policy prohibiting or restricting the use of its equipment for the initiation or delivery of unsolicited electronic mail advertisements.

(e) Nothing in this section shall be construed to limit or restrict the rights of an electronic mail service provider under Section 230(c)(1) of Title 47 of the United States Code, or any decision of an electronic mail service provider to permit or to restrict access to or use of its system, or any exercise of its editorial function.

(f) (1) In addition to any other action available under law, any electronic mail service provider whose policy on unsolicited electronic mail advertisements is violated as provided in this section may bring a civil action to recover the actual monetary loss suffered by that provider by reason of that violation, or liquidated damages of fifty dollars ($50) for each electronic mail message initiated or delivered in violation of this section, up to a maximum of twenty-five thousand dollars ($25,000) per day, whichever amount is greater.

Remedy: $50 per message initiated or delivered

(2) In any action brought pursuant to paragraph (1), the court may award reasonable attorney's fees to a prevailing party.

(3) (A) In any action brought pursuant to paragraph (1), the electronic mail service provider shall be required to establish as an element of its cause of action that prior to the alleged violation, the defendant had actual notice of both of the following:

(i) The electronic mail service provider's policy on unsolicited electronic mail advertising.
(ii) The fact that the defendant's unsolicited electronic mail advertisements would use or cause to be used the electronic mail service provider's equipment located in this state.

Plaintiff must show that defendant had actual ~~or~~ knowledge of policy + use of ISP equipment

(B) In this regard, the Legislature finds that with rapid advances in Internet technology, and electronic mail technology in particular, Internet service providers are already experimenting with embedding policy statements directly into the software running on the computers used to provide electronic mail services in a manner that displays the policy statements every time an electronic mail delivery is requested. While the state of the technology does not support such a finding at present, the Legislature believes that, in a given case at some future date, a showing that notice was supplied via electronic means between the sending and receiving computers could be held to constitute actual notice to the sender for purposes of this paragraph.

(4) A violation of this section shall not be subject to Section 17534.

SEC. 3. Section 502 of the Penal Code is amended to read:

502. (a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:

(1) "Access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

(2) "Computer network" means any system that provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication

facilities.

(3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.

(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(6) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

(7) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.

(8) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access.

(9) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

(10) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(11) "Internet domain name" means a globally unique, hierarchical reference to an Internet host or service, assigned through centralized Internet naming authorities, comprising a series of character strings separated by periods, with the rightmost character string specifying the top of the hierarchy.

(c) Except as provided in subdivision (h), any person who commits any of the following

acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

Anti forged headers.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

(d) (1) Any person who violates any of the provisions of paragraph (1), (2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:

(A) For the first violation that does not result in injury, and where the value of the computer services used does not exceed four hundred dollars ($400), by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000) or in an injury,

or if the value of the computer services used exceeds four hundred dollars ($400), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(3) Any person who violates paragraph (6), (7), or (8) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding two hundred fifty dollars ($250).

(B) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(4) Any person who violates paragraph (9) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding two hundred fifty dollars ($250).

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(e) (1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data may bring a civil action against any person convicted under this section for compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.

(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees to a prevailing party.

(3) A community college, state university, or academic institution accredited in this state is required to include computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a

resolution to that effect.

(f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

(g) Any computer, computer system, computer network, or any software or data, owned by the defendant, that is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture, as specified in Section 502.01.

(h) (1) Subdivision (c) does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or data when acting within the scope of his or her lawful employment.

(2) Paragraph (3) of subdivision (c) does not apply to any employee who accesses or uses his or her employer's computer system, computer network, computer program, or data when acting outside the scope of his or her lawful employment, so long as the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or so long as the value of supplies and computer services, as defined in paragraph (4) of subdivision (b), which are used do not exceed an accumulated total of one hundred dollars ($100).

(i) No activity exempted from prosecution under paragraph (2) of subdivision (h) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

(j) For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

(k) In determining the terms and conditions applicable to a person convicted of a violation of this section the court shall consider the following:

(1) The court shall consider prohibitions on access to and use of computers.
(2) Except as otherwise required by law, the court shall consider alternate sentencing, including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.

SEC. 4. No reimbursement is required by this act pursuant to Section 6 of Article XIIIB of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIIIB of the California Constitution.

Notwithstanding Section 17580 of the Government Code, unless otherwise specified, the provisions of this act shall become operative on the same date that the act takes effect pursuant to the California Constitution.

Assembly Bill No. 1676

CHAPTER 865

An act to amend Section 17538.4 of the Business and Professions Code, relating to advertising.

[Approved by Governor September 26, 1998. Filed with Secretary of State September 28, 1998.]

LEGISLATIVE COUNSEL'S DIGEST

AB 1676, Bowen. Advertising: electronic mail.

Existing law prohibits a person conducting business in this state from faxing unsolicited advertising material, unless certain conditions are satisfied.

This bill would expand that prohibition to include the transmission of unsolicited advertising by electronic mail (e-mail), and would make several related changes.

This bill would become inoperative if federal law on this subject is enacted.

Existing law provides for the regulation of advertising and provides that a violation of those provisions is a crime. This bill, by creating additional prohibitions with regard to advertising, would expand the scope of an existing crime, thereby imposing a state-mandated local program.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

The people of the State of California do enact as follows:

SECTION 1. Section 17538.4 of the Business and Professions Code is amended to read:

17538.4. (a) No person or entity conducting business in this state shall facsimile (fax) or cause to be faxed, or electronically mail (e-mail) or cause to be e-mailed, documents consisting of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit unless:

(1) In the case of a fax, that person or entity establishes a toll-free telephone number that a recipient of the unsolicited faxed documents may call to notify the sender not to fax the recipient any further unsolicited documents.

(2) In the case of e-mail, that person or entity establishes a toll-free telephone number or valid sender operated return e-mail address that the recipient of the unsolicited documents may call or e-mail to notify the sender not to e-mail any further unsolicited documents.

(b) All unsolicited faxed or e-mailed documents subject to this section shall include a statement informing the recipient of the toll-free telephone number that the recipient may call, or a valid return address to which the recipient may write or e-mail, as the case may be, notifying the sender not to fax or e-mail the recipient any further unsolicited documents to the fax number, or numbers, or e-mail address, or addresses, specified by the recipient.

In the case of faxed material, the statement shall be in at least nine-point type. In the case of e-mail, the statement shall be the first text in the body of the message and shall be of the same size as the majority of the text of the message.

(c) Upon notification by a recipient of his or her request not to receive any further unsolicited faxed or e-mailed documents, no person or entity conducting business in this state shall fax or cause to be faxed or e-mail or cause to be e-mailed any unsolicited documents to that recipient.

(d) In the case of e-mail, this section shall apply when the unsolicited e-mailed documents are delivered to a California resident via an electronic mail service provider's service or equipment located in this state. For these purposes "electronic mail service provider" means any business or organization qualified to do business in this state that provides individuals, corporations, or other entities the ability to send or receive electronic mail through equipment located in this state and that is an intermediary in sending or receiving electronic mail.

(e) As used in this section, "unsolicited e-mailed documents" means any e-mailed document or documents consisting of advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit that meet both of the following requirements:

(1) The documents are addressed to a recipient with whom the initiator does not have an existing business or personal relationship.

(2) The documents are not sent at the request of, or with the express consent of, the recipient.

(f) As used in this section, "fax" or "cause to be faxed" or "e-mail" or "cause to be e-mailed" does not include or refer to the transmission of any documents by a telecommunications utility or Internet service provider to the extent that the telecommunications utility or Internet service provider merely carries that transmission over its network.

(g) In the case of e-mail that consists of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit, the subject line of each and every message shall include "ADV:" as the first four characters.

mandatory disclosure of how to get out

def.

ISP safe harbor?

mandatory labeling

If these messages contain information that consists of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit, that may only be viewed, purchased, rented, leased, or held in possession by an individual 18 years of age and older, the subject line of each and every message shall include "ADV:ADLT" as the first eight characters.

(h) An employer who is the registered owner of more than one e-mail address may notify the person or entity conducting business in this state e-mailing or causing to be e-mailed, documents consisting of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit of the desire to cease e-mailing on behalf of all of the employees who may use employer-provided and employer-controlled e-mail addresses.

(i) This section, or any part of this section, shall become inoperative on and after the date that federal law is enacted that prohibits or otherwise regulates the transmission of unsolicited advertising by electronic mail (e-mail).

~~SEC. 2. No reimbursement is required by this act pursuant to~~ Section 6 of Article XIII B of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution.

Notwithstanding Section 17580 of the Government Code, unless otherwise specified, the provisions of this act shall become operative on the same date that the act takes effect pursuant to the California Constitution.

O

0084

Nevada Senate Bill No. 13

Introduced by Senator Raggio
Prefiled on January 14, 1997

As amended and passed by Assembly June 30, 1997 (third reprint)
Amended version concurred in by Senate July 1, 1997

AN ACT relating to actions concerning persons; providing that a person who transmits certain items of electronic mail is liable to the recipient for civil damages under certain circumstances; providing that the district court may enjoin a person from transmitting certain items of electronic mail under certain circumstances; and providing other matters properly relating thereto.

THE PEOPLE OF THE STATE OF NEVADA, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

Section 1 Chapter 41 of NRS is hereby amended by adding thereto the provisions set forth as sections 2 to 8, inclusive, of this act.

Sec. 2 *As used in sections 2 to 8, inclusive, of this act, unless the context otherwise requires, the words and terms defined in sections 3 to 6, inclusive, of this act have the meanings ascribed to them in those sections.*

Sec. 3 *"Advertisement" means material that:*

1. Advertises for commercial purposes the availability or the quality of real property, goods or services; or

2. Is otherwise designed or intended to solicit a person to purchase real property, goods or services.

Sec. 4 *"Electronic mail" means a message, a file or other information that is transmitted through a local, regional or global network, regardless of whether the message, file or other information is:*

1. Viewed;

2. Stored for retrieval at a later time;

3. Printed onto paper or other similar material; or

4. Filtered or screened by a computer program that is designed or intended to filter or screen items of electronic mail.

Sec. 5 *"Network" means a network comprised of one or more computers that may be accessed by a modem, electronic or optical technology or other similar means.*

Sec. 6 *"Recipient" means a person who receives an item of electronic mail.*

Sec. 7 *1. Except as otherwise provided in section 8 of this act, if a person transmits or causes to be transmitted to a recipient an item of electronic mail that includes an advertisement, the person is liable to the recipient for civil damages unless:*

(a) The person has a preexisting business or personal relationship with the recipient; or

(b) The recipient has expressly consented to receive the item of electronic mail from the person; or

(c) The advertisement is readily identifiable as promotional, or contains a statement providing that it is an advertisement, and clearly and conspicuously provides:

clearly promoted or contains disclaimer

(1) The legal name, complete street address and electronic mail address of the person transmitting the electronic mail; and

(2) A notice that the recipient may decline to receive additional electronic mail that includes an advertisement from the person transmitting the electronic mail and the procedures for declining such electronic mail.

2. If a person is liable to a recipient pursuant to subsection 1, the recipient may recover from the person:

(a) Actual damages or damages of $10 per item of electronic mail received, whichever is greater; and

(b) Attorney's fees and costs.

3. In addition to any other recovery that is allowed pursuant to subsection 2, the recipient may apply to the district court of the county in which the recipient resides for an order enjoining the person from transmitting to the recipient any other item of electronic mail that includes an advertisement.

Sec. 8 *1. If a person provides users with access to a network and, as part of that service, transmits items of electronic mail on behalf of those users, the person is immune from liability for civil damages pursuant to sections 2 to 8, inclusive, of this act, unless the person transmits an item of electronic mail that includes an advertisement he prepared or caused to be prepared.*

ISP not liable

2. The provisions of sections 2 to 8, inclusive, of this act do not apply to an item of electronic mail that is obtained by a recipient voluntarily. This subsection includes, but is not limited to, an item of electronic mail that is obtained by a recipient voluntarily from an electronic bulletin board.

Unsolicited e-mail legislation

Washington House Bill 2752 (1998) (as enacted)

State of Washington
55th Legislature
1998 Regular Session

ENGROSSED SUBSTITUTE HOUSE BILL 2752

By House Committee on Energy & Utilities (originally sponsored by Representatives Bush, Crouse, Gardner, Cairnes, Dyer, Mulliken, Morris, Linville, Reams, Romero, Smith, McDonald, Ogden, Dickerson, Butler, O'Brien, Ballasiotes, Talcott and Appelwick; by request of Attorney General)

Introduced January 19, 1998 [text as introduced]
(Companion bill SB 6434 also introduced January 19, 1998)
Substitute version passed House February 16, 1998
Passed Senate with amendments March 4, 1998
House concurred in Senate amendments March 7, 1998
Signed by Governor March 25, 1998; effective date: June 11, 1998

AN ACT Relating to electronic mail; adding a new chapter to Title 19 RCW; creating a new section; prescribing penalties; and providing an expiration date.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec. 1. The legislature finds that the volume of commercial electronic mail is growing, and the consumer protection division of the attorney general's office reports an increasing number of consumer complaints about commercial electronic mail. Interactive computer service providers indicate that their systems sometimes cannot handle the volume of commercial electronic mail being sent and that filtering systems fail to screen out unsolicited commercial electronic mail messages when senders use a third party's internet domain name without the third party's permission, or otherwise misrepresent the message's point of origin. The legislature seeks to provide some immediate relief to interactive computer service providers by prohibiting the sending of commercial electronic mail messages that use a third party's internet domain name without the third party's permission, misrepresent the message's point of origin, or contain untrue or misleading information in the subject line.**

The legislature also finds that the utilization of electronic mail messages for commercial purposes merits further study. A select task force should be created to explore technical, legal, and cost issues surrounding the usage of electronic mail messages for commercial purposes and to recommend to the legislature any potential legislation needed for regulating commercial electronic mail messages.

NEW SECTION. **Sec. 2. The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.**

(1) "Commercial electronic mail message" means an electronic mail message sent for the purpose of promoting real property, goods, or services for sale or lease.

~~**(2) "Electronic mail address" means a destination, commonly**~~

(2) "Electronic mail address" means a destination, commonly expressed as a string of characters, to which electronic mail may be sent or delivered.

(3) "Initiate the transmission" refers to the action by the original sender of an electronic mail message, not to the action by any intervening interactive computer service that may handle or retransmit the message.

(4) "Interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the internet and such systems operated or services offered by libraries or educational institutions.

(5) "Internet domain name" refers to a globally unique, hierarchical reference to an internet host or service, assigned through centralized internet naming authorities, comprising a series of character strings separated by periods, with the right-most string specifying the top of the hierarchy.

NEW SECTION. Sec. 3. (1) No person, corporation, partnership, or association may initiate the transmission of a commercial electronic mail message from a computer located in Washington or to an electronic mail address that the sender knows, or has reason to know, is held by a Washington resident that:

(a) Uses a third party's internet domain name without permission of the third party, or otherwise misrepresents any information in identifying the point of origin or the transmission path of a commercial electronic mail message; or

(b) Contains false or misleading information in the subject line.

(2) For purposes of this section, a person, corporation, partnership, or association knows that the intended recipient of a commercial electronic mail message is a Washington resident if that information is available, upon request, from the registrant of the internet domain name contained in the recipient's electronic mail address.

NEW SECTION. Sec. 4. (1) It is a violation of the consumer protection act, chapter 19.86 RCW, to initiate the transmission of a commercial electronic mail message that:

(a) Uses a third party's internet domain name without permission of the third party, or otherwise misrepresents any information in identifying the point of origin or the transmission path of a commercial electronic mail message; or

(b) Contains false or misleading information in the subject line.

(2) The legislature finds that the practices covered by this chapter are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. A violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW.

NEW SECTION. Sec. 5. (1) Damages to the recipient of a commercial electronic mail message sent in violation of this chapter are five hundred dollars, or actual damages, whichever is greater.

(2) Damages to an interactive computer service resulting from a violation of this chapter are one thousand dollars, or actual damages, whichever is greater.

NEW SECTION. Sec. 6. (1) An interactive computer service may, upon

its own initiative, block the receipt or transmission through its service of any commercial electronic mail that it reasonably believes is, or will be, sent in violation of this chapter.

(2) No interactive computer service may be held liable for any action voluntarily taken in good faith to block the receipt or transmission through its service of any commercial electronic mail which it reasonably believes is, or will be, sent in violation of this chapter.

~~NEW SECTION. Sec. 7. Sections 1 through 6 of this act constitute a new~~ chapter in Title 19 RCW.

NEW SECTION. Sec. 8. (1) The select task force on commercial electronic mail messages is hereby created. The select task force shall:

(a) Identify technical, legal, and cost issues in relation to the transmission and receipt of commercial electronic mail messages over the internet;

(b) Evaluate whether existing laws are sufficient to resolve any technical, legal, or financial problems created by the increasing volume of commercial electronic mail messages;

(c) Review efforts being made by the federal government and other states to regulate the transmission of commercial electronic mail messages; and

(d) Prepare a report identifying policy options and recommendations for any potential legislation needed to regulate commercial electronic mail messages. The report shall be delivered to the house of representatives energy and utilities committee by November 15, 1998.

(2) The select task force shall be composed of five members, consisting of:

(a) Two members of the house of representatives, one from each of the two largest caucuses, each member being a member of the house of representatives energy and utilities committee, appointed by the speaker of the house of representatives;

(b) Two members of the senate, one from each of the two largest caucuses, each member being a member of the senate energy and utilities committee, appointed by the president; and

(c) One person appointed by the governor.

(3) The select task force shall solicit input from interested parties, including but not limited to, persons representing:

(a) Attorney general's consumer protection division;

(b) Internet service providers;

(c) Direct marketers;

(d) Manufacturers of electronic mail messaging software;

(e) Nonprofit organizations interested in free speech and other civil liberty matters; and

(f) Internet users.

(4) Staff support for the select task force shall be provided by the house of representatives office of program research and senate committee services.

(5) ~~This section expires December 31, 1998.~~

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

CompuServe Incorporated, Plaintiff,
vs.
Cyber Promotions, Inc. and Sanford Wallace, Defendants.

Case No. C2-96-1070
JUDGE GRAHAM

February 3, 1997

MEMORANDUM OPINION AND ORDER

This case presents novel issues regarding the commercial use of the Internet, specifically the right of an online computer service to prevent a commercial enterprise from sending unsolicited electronic mail advertising to its subscribers.

Plaintiff CompuServe Incorporated ("CompuServe") is one of the major national commercial online computer services. It operates a computer communication service through a proprietary nationwide computer network. In addition to allowing access to the extensive content available within its own proprietary network, CompuServe also provides its subscribers with a link to the much larger resources of the Internet. This allows its subscribers to send and receive electronic messages, known as "e-mail," by the Internet. Defendants Cyber Promotions, Inc. and its president Sanford Wallace are in the business of sending unsolicited e-mail advertisements on behalf of themselves and their clients to hundreds of thousands of Internet users, many of whom are CompuServe subscribers. CompuServe has notified defendants that they are prohibited from using its computer equipment to process and store the unsolicited e-mail and has requested that they terminate the practice. Instead, defendants have sent an increasing volume of e-mail solicitations to CompuServe subscribers. CompuServe has attempted to employ technological means to block the flow of defendants' e-mail transmissions to its computer equipment, but to no avail.

This matter is before the Court on the application of CompuServe for a preliminary injunction which would extend the duration of the temporary restraining order issued by this Court on October 24, 1996 and which would in addition prevent defendant from sending unsolicited advertisements to CompuServe subscribers.

For the reasons which follow, this Court holds that where defendants engaged in a course of conduct of transmitting a substantial volume of electronic data in the form of unsolicited e-mail to plaintiff's proprietary computer equipment, where defendants continued such practice after repeated demands to cease and desist, and where defendants deliberately evaded plaintiff's affirmative efforts to protect its computer equipment from such use, plaintiff has a viable claim for trespass to personal property and is entitled to injunctive relief to protect its property.

I.

The Court will begin its analysis of the issues by acknowledging, for the purpose of providing a background, certain findings of fact recently made by another district court in a case involving the Internet:

> 1. The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks. . . .

> 2. Some networks are "closed" networks, not linked to other computers or networks. Many networks, however, are connected to other networks, which are in turn connected to other networks in a manner which permits each computer in any network to communicate with computers on any other network in the system. This global Web of linked networks and computers is referred to as the Internet.
>
> 3. The nature of the Internet is such that it is very difficult, if not impossible, to determine its size at a given moment. It in indisputable, however, that the Internet has experienced extraordinary growth in recent years. . . . In all, reasonable estimates are that as many as 40 million people around the world can and do access the enormously flexible communication Internet medium. That figure is expected to grow to 200 million Internet users by the year 1999.
>
> 4. Some of the computers and computer networks that make up the network are owned by governmental and public institutions, some are owned by non-profit organizations, and some are privately owned. The resulting whole is a decentralized, global medium of communications -- or "cyberspace" -- that links people, institutions, corporations, and governments around the world. . . .
>
> . . . .
>
> 11. No single entity -- academic, corporate, governmental, or non-profit administers the Internet. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers). There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet.

American Civil Liberties Union v. Reno, 929 F. Supp. 824, 830-832 (E.D. Pa. 1996). In 1994, one commentator noted that "advertisements on the current Internet computer network are not common because of the network's not-for-profit origins." Trotter Hardy, *The Proper Legal Regime for "Cyberspace",* 55 U. Pitt. L. Rev. 993, 1027 (1994). In 1997, that statement is no longer true.

Internet users often pay a fee for Internet access. However there is no per-message charge to send electronic messages over the Internet and such messages usually reach their destination within minutes. Thus electronic mail provides an opportunity to reach a wide audience quickly and at almost no cost to the sender. It is not surprising therefore that some companies, like defendant Cyber Promotions, Inc., have begun using the Internet to distribute advertisements by sending the same unsolicited commercial message to hundreds of thousands of Internet users at once. Defendants refer to this as "bulk e-mail," while plaintiff refers to it as "junk e-mail." In the vernacular of the Internet, unsolicited e-mail advertising is sometimes referred to pejoratively as "spam."[1]

[1] This term is derived from a skit performed on the British television show Monty Python's Flying Circus, in which the word "spam" is repeated to the point of absurdity in a restaurant menu.

CompuServe subscribers use CompuServe's domain name "CompuServe.com" together with their own unique alphanumeric identifier to form a distinctive e-mail mailing address. That address may be used by the subscriber to exchange electronic mail with any one of tens of millions of other Internet users who have electronic mail capability. E-mail sent to CompuServe subscribers is processed and stored on CompuServe's proprietary computer equipment. Thereafter, it becomes accessible to CompuServe's subscribers, who can access CompuServe's equipment and electronically retrieve those messages.

Over the past several months, CompuServe has received many complaints from subscribers threatening to discontinue their subscription unless CompuServe prohibits electronic mass mailers from

using its equipment to send unsolicited advertisements. CompuServe asserts that the volume of messages generated by such mass mailings places a significant burden on its equipment which has finite processing and storage capacity. CompuServe receives no payment from the mass mailers for processing their unsolicited advertising. However, CompuServe's subscribers pay for their access to CompuServe's services in increments of time and thus the process of accessing, reviewing and discarding unsolicited e-mail costs them money, which is one of the reasons for their complaints. CompuServe has notified defendants that they are prohibited from using its proprietary computer equipment to process and store unsolicited e-mail and has requested them to cease and desist from sending unsolicited e-mail to its subscribers. Nonetheless, defendants have sent an increasing volume of e-mail solicitations to CompuServe subscribers.

In an effort to shield its equipment from defendants' bulk e-mail, CompuServe has implemented software programs designed to screen out the messages and block their receipt. In response, defendants have modified their equipment and the messages they send in such a fashion as to circumvent CompuServe's screening software. Allegedly, defendants have been able to conceal the true origin of their messages by falsifying the point-of-origin information contained in the header of the electronic messages. Defendants have removed the "sender" information in the header of their messages and replaced it with another address. Also, defendants have developed the capability of configuring their computer servers to conceal their true domain name and appear on the Internet as another computer, further concealing the true origin of the messages. By manipulating this data, defendants have been able to continue sending messages to CompuServe's equipment in spite of CompuServe's protests and protective efforts.

Defendants assert that they possess the right to continue to send these communications to CompuServe subscribers. CompuServe contends that, in doing so, the defendants are trespassing upon its personal property.

II.

The grant or denial of a motion for preliminary injunction rests within the discretion of the trial court. *Deckert v. Independence Shares Corp.*, 311 U.S. 282 (1940). In determining whether a motion for preliminary injunction should be granted, a court must consider and balance four factors: (1) the likelihood that the party seeking the preliminary injunction will succeed on the merits of the claim; (2) whether the party seeking the injunction will suffer irreparable harm without the grant of the extraordinary relief; (3) the probability that granting the injunction will cause substantial harm to others; and (4) whether the public interest is advanced by the issuance of the injunction. *Washington v. Reno*, 35 F.3d 1093, 1099 (6th Cir. 1994); *International Longshoremen's Assoc. v. Norfolk S. Corp.*, 927 F.2d 900, 903 (6th Cir. 1991). None of these individual factors constitute prerequisites that must be met for the issuance of a preliminary injunction, they are instead factors that are to be balanced. *In re DeLorean Motor Co.*, 755 F.2d 1223, 1229 (6th Cir. 1985). A preliminary injunction is customarily granted on the basis of procedures that are less formal and evidence that is less complete than in a full trial on the merits. Indeed, "[a] party . . . is not required to prove his case in full at a preliminary injunction hearings." *University of Texas v. Camenisch*, 451 U.S. 390, 395 (1981).

III.

This court shall first address plaintiff's motion as it relates to perpetuating the temporary restraining order filed on October 24, 1996. That order enjoins defendants from:

> (i) Using CompuServe accounts or CompuServe's equipment or support services to send or receive electronic mail or messages or in connection with the sending or receiving of electronic mail or messages;
>
> (ii) Inserting any false reference to a CompuServe account or CompuServe account or equipment in any electronic message sent by Defendants; and
>
> (iii) Falsely representing or causing their electronic mail or messages to bear the representation that any electronic mail or message sent by Defendants was sent by or

representation that any electronic mail or message sent by Defendants was sent by or originated from CompuServe or a CompuServe account.

(Temporary Restraining Order at 4).

As a general matter, the findings of this Court enunciated in its temporary restraining order are applicable to the request for preliminary injunction now at issue. The behavior described in subsections (ii) and (iii) of the temporary restraining order would be actionable as false representations or descriptions under §43(a) of the Lanham Act, 15 U.S.C. §1125(a). Also, the same behavior is actionable under the Ohio Deceptive Trade Practices Act, Ohio Rev. Code §4165(B) and (D).

Defendants argue that the restrictions in the temporary restraining order are no longer necessary because defendants no longer have a CompuServe account. That being the case, a preliminary injunction perpetuating the prescribed activity articulated in subsection (i) of the temporary restraining order will present no hardship at all to defendants. Next, it does not appear that defendants would need to have a CompuServe account to perpetrate the prescribed acts articulated in subsections (ii) and (iii) of the temporary restraining order. Therefore, the fact that defendants no longer have an account with plaintiff does not vitiate the need which CompuServe has demonstrated for an injunction prescribing the acts set forth in those subsections.

For the foregoing reasons and the reasons articulated in the temporary restraining order issued by this Court, defendants Cyber Promotions, Inc. and its president Sanford Wallace are hereby enjoined from performing any of the acts therein described during the pendency of this litigation.

IV.

This Court will now address the second aspect of plaintiff's motion in which it seeks to enjoin defendants Cyber Promotions, Inc. and its president Sanford Wallace from sending any unsolicited advertisements to any electronic mail address maintained by CompuServe.

CompuServe predicates this aspect of its motion for preliminary injunction on the common law theory of trespass to personal property or to chattels, asserting that defendants continued transmission of electronic messages to its computer equipment constitutes an actionable tort.

Trespass to chattels has evolved from its original common law application, concerning primarily the asportation of another's tangible property, to include the unauthorized use of personal property.

> Its chief importance now, is that there may be recovery. . . . for interferences with the possession of chattels which are not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered. Trespass to chattels survives today, in other words, largely as a little brother of conversion.

Prosser & Keeton, *Prosser and Keeton on Torts,* §14, 85-86 (1984).

The scope of an action for conversion recognized in Ohio may embrace the facts in the instant case. The Supreme Court of Ohio established the definition of conversion under Ohio law in *Baltimore & O.R. Co. v. O'Donnell,* 49 Ohio St. 489, 32 N.E. 476, 478 (1892) by stating that:

> [I]n order to constitute a conversion, it was not necessary that there should have been an actual appropriation of the property by the defendant to its own use and benefit. It might arise from the exercise of a dominion over it in exclusion of the rights of the owner, or withholding it from his possession under a claim inconsistent with his rights. If one take the property of another, for a temporary purpose only, in disregard of the owner's right, it is a conversion. Either a wrongful taking, an assumption of ownership, an illegal use or misuse, or a wrongful detention of chattels will constitute a conversion.

Id. at 497-98, *see also Miller v. Uhl,* 37 Ohio App. 276, 174 N.B. 591 (1929); *Great American Mut.*

Indem. Co. v. Meyer, 18 Ohio App. 97 (1924); 18 O. Jur. 3d, Conversion §17. While authority under Ohio law respecting an action for trespass to chattels is extremely meager, it appears to be an actionable tort. *See State of Ohio v. Herbert,* 49 Ohio St. 2d 88, 119, 358 N.E. 2d 1090, 1106 (1976) (dissenting opinion) ("any workable cause of action would appear to be trespass to chattels"); *see also Greenwald v. Kearns,* 104 Ohio App. 473, 145 N.E. 2d 462 (1957) (trespass on the rights of plaintiff in personal property is a precursor to an act in conversion); *Simmons v. Dimitrouleas Wallcovering, Inc.,* No. 14804, 1995 WL 19136, at *2 (Ohio App. Jan. 18, 1995) (the court of appeals acknowledged that trespass to chattel claims were barred because those claims were dependent upon claimant's ownership of the subject personal property); *Klienbriel v. Smith,* No. 94CA1641, 1996 WL 57947, at *2 (Ohio App. Feb. 6, 1996) (where the court of appeals let stand a jury award on a "trespass against personal property" claim); *Springfield Bank v. Casserta,* 10 B.R. 57 (Bankr. S.D. Ohio 1981) (common law principles of trespass to chattels in Am. Jur. 2d applied as controlling under Ohio law).

Both plaintiff and defendants cite the Restatement (Second) of Torts to support their respective positions. In determining a question unanswered by state law, it is appropriate for this Court to consider such sources as the restatement of the law and decisions of other jurisdictions. *Bailey v. V & O Press Co., Inc.,* 770 F.2d 601, 604-606 (6th Cir. 1985) (where court considered positions expressed in the Restatement (Second) of Torts in interpreting Ohio's principles of comparative negligence); *Garrison v. Jervis B. Webb Co.,* 583 F.2d 258, 262 n. 6 (1978); *see also* Wright, Miller & Cooper, *Federal Practice and Procedure,* §4507 (West 1996).

The Restatement §217(b) states that a trespass to Chattel may be committed by intentionally using or intentionally using or intermeddling with the chattel in possession of another. Restatement §217, Comment e defines physical "intermeddling" as follows:

> . . . intentionally bringing about a physical contact with the chattel. The actor may commit a trespass by an act which brings him into an intended physical contact with a chattel in the possession of another[.]

Electronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action. *Thrifty-Tel, Inc. v. Bezeneck,* 56 Cal. App. 4th 1559, 1567 (1996); *State v. McGraw,* 480 N.E. 2d 552, 554 (Ind. 1985) (Indiana Supreme Court recognizing in dicta that a hacker's unauthorized access to a Computer was more in the nature of trespass than criminal conversion); and *State v. Riley,* 121 Wash. 2d 22, 846 P.2d 1365 (1993) (computer hacking as the criminal offense of "computer trespass" under Washington law). It is undisputed that plaintiff has a possessory interest in its computer systems. Further, defendants' contact with plaintiff's computers is clearly intentional. Although electronic messages may travel through the Internet over various routes, the massages are affirmatively directed to their destination.

Defendants, citing Restatement (Second) of Torts §221, which defines "disposition", assert that not every interference with the personal property of another is actionable and that physical dispossession or substantial interference with the chattel is required. Defendants then argue that they did not, in this case, physically dispossess plaintiff of its equipment or substantially interfere with it. However, the Restatement (Second) of Torts §218 defines the circumstances under which a trespass to chattels may be actionable:

> One who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,
>
> (a) he dispossessed the other of the chattel, or
>
> (b) the chattel is impaired as to its condition, quality, or value, or
>
> (c) the possessor is deprived of the use of the chattel for a substantial time, or
>
> (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.

Therefore, an interference resulting in physical dispossession is in just one circumstance under which a defendant can be found liable. Defendants suggest that "[u]nless an alleged trespasser actually takes physical custody of the property or physically damages it, courts will not find the 'substantial interference' required to maintain a trespass to chattel claim." (Defendant's Memorandum at 13). To support this rather broad proposition, defendants cite only two cases which make any reference to the Restatement. In *Glidden v. Szybiak,* 95 N.H. 318, 63 A.2d 233 (1949), the court simply indicated that an action for trespass to chattels could not be maintained in the absence of some form of damage. The court held that where plaintiff did not contend that defendant's pulling on her pet dog's ears caused any injury, an action in tort could not be maintained. *Id.* at 235. In contrast, plaintiff in the present action has alleged that it has suffered several types of injury as a result of defendants' conduct. In *Koepnick v. Sears Roebuck & Co.,* 158 Ariz. 322, 762 P.2d 609 (1988) the court held that a two-minute search of an individual's truck did not amount to a "dispossession" of the truck as defined in Restatement §221 or a deprivation of the use of the truck for a substantial time. It is clear from a reading of Restatement §218 that an interference or intermeddling that does not fit the §221 definition of "dispossession" can nonetheless result in defendants', liability for trespass. The *Koepnick* court did not discuss any of the other grounds for liability under Restatement §218.

A plaintiff can sustain an action for trespass to chattels, as opposed to an action for conversion, without showing a substantial interference with its right to possession of that chattel. *Thrifty-Tel, Inc.,* 46 Cal. App. 4th at 1567 (quoting *Zaalow v. Kroenert,* 29 Cal. 2d 541, 176 P.2d 1 (Cal. 1946)). Harm to the personal property or diminution of its quality, condition, or value as a result of defendants' use can also be the predicate for liability. Restatement §218(b).

> An unprivileged use or other intermeddling with a chattel which results in actual impairment of its physical condition, quality or value to the possessor makes the actor liable for the loss thus caused. In the great majority of cases, the actor's intermeddling with the chattel impairs the value of it to the possessor, as distinguished from the mere affront to his dignity as possessor, only by some impairment of the physical condition of the chattel. There may, however, be situations in which the value to the owner of a particular type of chattel may be impaired by dealing with it in a manner that does not affect its physical condition. . . . In such a case, the intermeddling is actionable even though the physical condition of the chattel is not impaired.

The Restatement (Second) of Torts §218, comment h. In the present case, any value CompuServe realizes from its computer equipment is wholly derived from the extent to which that equipment can serve its subscriber base. Michael Mangino, a software developer for CompuServe who monitors its mail processing computer equipment states by affidavit that handling the enormous volume of mass mailings that CompuServe receives places a tremendous burden on its equipment. (Mangino Supp. Dec. at ¶12). Defendants' more recent practice of evading CompuServe's filters by disguising the origin of their messages commandeers even more computer resources because CompuServe computers are forced to store undeliverable e-mail messages and labor in vain to return the messages to an address that does not exist. (Mangino Supp. Dec. at ¶¶7-8). To the extent that defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's computer equipment, those resources are not available to serve CompuServe subscribers. Therefore, the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendants' conduct.

Next, plaintiff asserts that it has suffered injury aside from the physical impact of defendants' messages on its equipment. Restatement §218(d) also indicates that recovery may be had for a trespass that causes harm to something in which the possessor has a legally protected interest. Plaintiff asserts that defendants' messages are largely unwanted by its subscribers, who pay incrementally to access their e-mail, read it, and discard it. Also, the receipt of a bundle of unsolicited messages at once can require the subscriber to sift through, at his expense, all of the messages in order to find the ones he wanted or expected to receive. These inconveniences decrease the utility of CompuServe's e-mail service and are the foremost subject in recent complaints from CompuServe subscribers. Patrick Hole, a customer service manager for plaintiff, states by affidavit that in November 1996 CompuServe received approximately 9,970 e-mail complaints from subscribers about junk e-mail, a figure up from

approximately two hundred complaints the previous year. (Hole 2d Supp. Dec. at ¶4). Approximately fifty such complaints per day specifically reference defendants. (Hole Supp. Dec. at ¶3). Defendants contend that CompuServe subscribers are provided with a simple procedure to remove themselves from the mailing list. However, the removal procedure must be performed by the e-mail recipient at his expense, and some CompuServe subscribers complain that the procedure is inadequate and ineffectual. (See, e.g., Hole Supp. Dec. at ¶8).

Many subscribers have terminated their accounts specifically because of the unwanted receipt of bulk e-mail messages. (Hole Supp. Dec. at ¶9, Hole 2d Supp. Dec. at ¶6). Defendants' intrusions into CompuServe's computer systems, insofar as they harm plaintiff's business reputation and goodwill with its customers, are actionable under Restatement §218(d).

The reason that the tort of trespass to chattels requires some actual damage as a *prima facie* element, whereas damage is assumed where there is a trespass to real property, can be explained as follows:

> The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. Therefore, one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected as stated in Clause (c). *Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.*

Restatement (Second) of Torts §218, Comment e (emphasis added). Plaintiff CompuServe has attempted to exercise this privilege to protect its computer systems. However, defendant's affirmative efforts to evade plaintiff's security measures have circumvented any protection those self-help measures might have provided. In this case CompuServe has alleged and supported by affidavit that it has suffered several types of injury as a result of defendants' conduct. The foregoing discussion simply underscores that the damage sustained by plaintiff is sufficient to sustain an action for trespass to chattels. However, this Court also notes that the implementation of technological means of self- help, to the extent that reasonable measures are effective, is particularly appropriate in this type of situation and should be exhausted before legal action is proper.

Under Restatement §252, the owner of personal property can create a privilege in the would-be trespasser by granting consent to use the property. A great portion of the utility of CompuServe's e-mail service is that it allows subscribers to receive messages from individuals and entities located anywhere on the Internet. Certainly, then, there is at least a tacit invitation for anyone on the Internet to utilize plaintiff's computer equipment to send e-mail to its subscribers.[2] *Buchanan Marine, Inc. v. McCormack Sand Co.*, 743 F. Supp. 139 (E.D.N.Y. 1990) (whether there is consent to community use is a material issue of fact in an action for trespass to chattels). However, in or around October 1995, CompuServe employee Jon Schmidt specifically told Mr. Wallace that he was "prohibited from using CompuServe's equipment to send his junk e-mail messages." (Schmidt Dec. at ¶5). There is apparently some factual dispute as to this point, but it is clear from the record that Mr. Wallace became aware at about th is time that plaintiff did not want to receive messages from Cyber Promotions and that plaintiff was taking steps to block receipt of those messages. (Transcript of December 15, 1996 Hearing at 81-86).

[2] That consent is apparently subject to express limitations. See Kolehmainen Dec. at ¶2 and discussion *infra.*

Defendants argue that plaintiff made the business decision to connect to the Internet and that therefore it cannot now successfully maintain an action for trespass to chattels. Their argument is analogous to the argument that because an establishment invites the public to enter its property for business purposes, it cannot later restrict or revoke access to that property, a proposition which is erroneous under Ohio law. *See, e.g., State v. Carriker,* 5 Ohio App. 2d 255, 214 N.E. 2d 809 (1964) (the

law in Ohio is that a business invitee's privilege to remain on the premises of another may be revoked upon the reasonable notification to leave by the owner or his agents); *Allstate Ins. Co. v. U.S. Associates Realty, Inc.*, 11 Ohio App. 3d 242, 464 N.E. 2d 169 (1983) (notice of express restriction or limitation on invitation turns business invitee into trespasser). On or around October 1995, CompuServe notified defendants that it no longer consented to the use of its proprietary computer equipment. Defendants' continued use thereafter was a trespass. Restatement (Second) of Torts §§252 and 892A(5); *see also* Restatement (Second) of Torts §217, Comment f ("The actor may commit a new trespass by continuing an intermeddling which he has already begun, with or without the consent of the person in possession. Such intermeddling may persist after the other's consent, originally given, has been terminated."); Restatement (Second) of Torts §217, Comment g.

Further, CompuServe expressly limits the consent it grants to Internet users to send e-mail to its proprietary computer systems by denying unauthorized parties the use of CompuServe equipment to send unsolicited electronic mail messages. (Kolehmainen Dec. at ¶2). This policy statement, posted by CompuServe online, states as follows:

> CompuServe is a private online and communications services company. CompuServe does not permit its facilities to be used by unauthorized parties to process and store unsolicited e-mail. If an unauthorized party attempts to send unsolicited messages to e-mail addresses on a CompuServe service, CompuServe will take appropriate action to attempt to prevent those messages from being processed by CompuServe. Violations of CompuServe's policy prohibiting unsolicited e-mail should be reported to . . . .

Id. at ¶¶2 and 3. Defendants Cyber Promotions, Inc. and its president Sanford Wallace have used plaintiff's equipment in a fashion that exceeds that consent. The use of personal property exceeding consent in a trespass. *City of Amsterdam v. Daniel Goldreyer, Ltd.*, 882 F. Supp. 1273 (E.D.N.Y. 1995); Restatement (Second) of Torts §256. It is arguable that CompuServe's policy statement, insofar as it may serve as a limitation upon the scope of its consent to the use of its computer equipment, may be insufficiently communicated to potential third-party users when it is merely posted at some location on the network. However, in the present case the record indicates that defendants were actually notified that they were using CompuServe's equipment in an unacceptable manner. To prove that a would-be trespasser acted with the intent required to support liability in tort it is crucial that defendant be placed on notice that he is trespassing.

As a general matter, the public possesses a privilege to reasonably use the facilities of a public utility, Restatement (Second) of Torts §259, but Internet service providers have been held not to be common carriers. *Religious Technology Center v. Netcom On-Line Communications Services, Inc.*, 907 F. Supp. 1361 (N.D.Cal. 1995). The definition of public utility status under Ohio law was recently articulated in *A & B Refuse Disposers, Inc. v. Bd. of Ravenna Township Trustees*, 64 Ohio St. 3d 385, 596 N.E. 2d 423 (1992). The Ohio Supreme Court held that the determination of whether an entity is a "public utility" requires consideration of several factors relating to the "public service" and "public concern" characteristics of a public utility. *Id.* at 426. The public service characteristic contemplates an entity which devotes an essential good or service to the general public which the public in turn has a legal right to demand or receive. *Id.* at 425. CompuServe's network, Internet access and electronic mail services are simply not essential to society. There are many alternative forms of communication which are customarily used for the same purposes. Further, only a minority of society at large has the equipment to send and receive e-mail messages via the Internet, and even fewer actually do. The second characteristic of a public utility contemplates an entity which conducts its operations in such manner as to be a matter of public concern, that is, a public utility normally occupies a monopolistic or ogopolistic position in the relevant marketplace. *Id.* at 425-426. Defendants estimate that plaintiff serves some five million Internet users worldwide. However, there are a number of major Internet service providers that have very large subscriber bases, and with a relatively minor capital investment, anyone can acquire the computer necessary to provide Internet access services on a smaller scale. Furthermore, Internet users are not a "captive audience" to any single service provider, but can transfer from one service to another until they find one that best suits their needs. Finally, the Ohio Supreme Court made clear that a party asserting public utility status is required to support that assertion with evidence going to the relevant aforementioned factors. *Id.* at 427. Defendants have not argued that CompuServe is a public utility,

much less produced evidence tending to support such a conclusion. Therefore, CompuServe is not a public utility as that status is defined under Ohio law and defendants can not be said to enjoy a special privilege to use CompuServe's proprietary computer systems.

In response to the trespass claim, defendants argue that they have the right to continue to send unsolicited commercial e-mail to plaintiff's computer systems under the First Amendment to the United States Constitution. The First Amendment states that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press." The United States Supreme Court has recognized that "the constitutional guarantee of free speech is a guarantee only against abridgement by government, federal or state." *Hudgens v. NLRB,* 424 U.S. 507, 513 (1976). Indeed, the protection of the First Amendment is not a shield against "merely private conduct." *Hurley v. Irish- American Gay Group of Boston,* --- U.S. ---, ---, 115 S.Ct. 2338, 2344 (1995) (citation omitted).

Very recently, in an action filed by Cyber Promotions, Inc. against America Online, Inc. ("AOL") the United States District Court for the Eastern District of Pennsylvania held that AOL, a company selling services that are similar to those of CompuServe, is a private actor. *Cyber Promotions, Inc. v. America Online, Inc.,* 1996 WL 633702, *9 (E.D.Pa. 1996). That case involved the question of whether Cyber Promotions had the First Amendment right to send unobstructed e-mail to AOL subscribers. The court held that Cyber Promotions had no such right and that, inter alia, AOL was not exercising powers that are traditionally the exclusive prerogative of the state, such as where a private company exercises municipal powers by running a company town. *Id.* at *7; *Blum v. Yaretsky,* 457 U.S. 991, 1004-05 (1982); *Marsh v. Alabama,* 326 U.S. 501 (1946). This Court agrees with the conclusions reached by the United States District Court for the Eastern District of Pennsylvania.

In the present action, CompuServe is a private company. Moreover, the mere judicial enforcement of neutral trespass laws by the private owner of property does not alone render it a state actor. Rotunda & Nowak, *Treatise on Constitutional Law* §16.3, 546 (West 1992). Defendants do not argue that CompuServe is anything other than a private actor. Instead, defendants urge that because CompuServe is so intimately involved in this new medium it might be subject to some special form of regulation. Defendants cite *Associated Press v. United States,* 326 U.S. 1 (1945), and *Turner Broadcasting Sys., Inc. v. FCC,* --- U.S. ---, 114 S. Ct. 2445 (1994), which stand for the proposition that when a private actor has a certain quantum of control over a central avenue of communication, then the First Amendment might not prevent the government from enacting legislation requiring public access to private property. No such legislation yet exists that is applicable to CompuServe. Further, defendants discussion concerning the extent to which the Internet may be regulated (or should be regulated) is irrelevant because no government entity has undertaken to regulate the Internet in a manner that is applicable to this action. Indeed, if there were some applicable statutory scheme in place this Court would not be required to apply paradigms of common law to the case at hand.

In *Lloyd Corp. v. Tanner,* 407 U.S. 551 (1972), protestors of the Vietnam War sought to pass out written materials in a private shopping center. Even though the customers of the shopping center were the intended recipients of the communication, the Supreme Court held that allowing the First Amendment to trump private property rights is unwarranted where there are adequate alternative avenues of communication. *Id.* at 567. The Supreme Court stated that:

> Although . . . the courts properly have shown a special solicitude for the guarantees of the First Amendment, *this Court has never held that a trespasser or an uninvited guest may exercise general rights of free speech on property privately owned and used nondiscriminatorily for private purposes only.*

Id. at 567-68 (emphasis added). Defendants in the present action have adequate alternative means of communication available to them. Not only are they free to send e-mail advertisements to those on the Internet who do not use CompuServe accounts, but they can communicate to CompuServe subscribers as well through online bulletin boards, web page advertisements, or facsimile transmissions, as well as through more conventional means such as the U.S. mail or telemarketing. Defendants' contention, referring to the low cost of the electronic mail medium, that there are no *adequate* alternative means of

communication is unpersuasive. There is no constitutional requirement that the incremental cost of sending massive quantities of unsolicited advertisements must be borne by the recipients. The legal concept in Lloyd that private citizens are entitled to enforce laws of trespass against would-be communicators is applicable to this case.

Defendants assert that CompuServe has assumed the role of postmaster, to whom all of the strictures of the First Amendment apply, and that to allow it to enjoy a legally protected interest in its computer equipment in this context is to license a form of censorship which violates the First Amendment. However, such an assertion must be accompanied by a showing that CompuServe is a state actor. An earlier mentioned, defendants have neither specifically argued this point nor provided any evidence to support it. CompuServe is entitled to restrict access to its private property.

"The First and Fourteenth Amendments have never been treated as absolutes. Freedom of speech or press does not mean that one can talk or distribute where, when and how one chooses. *Breard v. City of Alexandria,* 341 U.S. 622, 642 (1951) (upholding local ordinances banning commercial solicitations over First Amendment objections) (footnote omitted). In *Rowan v. U.S. Post Office Dept.,* 397 U.S. 728 (1970) the United States Supreme Court held that the First Amendment did not forbid federal legislation that allowed addressees to remove themselves from mailing lists and stop all future mailings. The Court stated that the "mailer's right to communicate must stop at the mailbox of an unreceptive addressee. . . . [t]o hold less would be to license a form of trespass[.]" *Id.* at 736-37.

In *Tillman v. Distribution Sys. of America, Inc.,* 648 N.Y.S.2d 630 (N.Y.A.D. 1996) the plaintiff complained that the defendant continued to throw newspapers on his property after being warned not to do so. The court held that the defendant newspaper distributor had no First Amendment right to continue to throw newspapers onto the property of the plaintiff. After discussing the Supreme Court cases of *Rowan* and *Breard, supra,* the court pointed out that:

> The most critical and fundamental distinction between the cases cited above, on the one hand, and the present case, on the other, is based on the fact that here we are not dealing with a government agency which seeks to preempt in some way the ability of a publisher to contact a potential reader; rather, we are dealing with a reader who is familiar with a publisher's product, and who is attempting to prevent the unwanted dumping of this product on his property. None of the cases cited by the defendants stands for the proposition that the Free Speech Clause prohibits such a landowner from resorting to his common-law remedies in order to prevent such unwanted dumping. There is, in our view, nothing in either the Federal or State Constitutions which requires a landowner to tolerate a trespass whenever the trespasser is a speaker, or the distributor of written speech, who is unsatisfied with the fora which may be available on public property, and who thus attempts to carry his message to private property against the will of the owner.

Id. at 635. The court concluded, relying on *Lloyd, supra,* that the property rights of the private owner could not be overwhelmed by the First Amendment. *Id.* at 636.

In the present case, plaintiff is physically the recipient of the defendants' messages and is the owner of the property upon which the transgression is occurring. As has been discussed, plaintiff is not a government agency or state actor which seeks to preempt defendants' ability to communicate but is instead a private actor trying to tailor the nuances of its service to provide the maximum utility to its customers.

Defendants' intentional use of plaintiff's proprietary computer equipment exceeds plaintiff's consent and, indeed, continued after repeated demands that defendants cease. Such use is an actionable trespass to plaintiff's chattel. The First Amendment to the United States Constitution provides no defense for such conduct.

Plaintiff has demonstrated a likelihood of success on the merits which is sufficient to warrant the issuance of the preliminary injunction it has requested.

As already discussed at some length, plaintiff has submitted affidavits supporting its contention that it will suffer irreparable harm without the grant of the preliminary injunction. As an initial matter, it is important to point out that the Court may accept affidavits as evidence of irreparable harm. *Wounded Knee Legal Defense/Offense Committee v. Federal Bureau of Investigation,* 507 F.2d 1281, 1287 (8th Cir. 1984); *see generally* Wright, Miller & Kane, *Federal Practice and Procedure* §2949, at 218-220 (West 1995). Defendants suggest that there are other reasons why CompuServe subscribers terminate their accounts, but do not offer any evidence which contradicts plaintiff's affidavits.

Normally, a preliminary injunction in not appropriate where an ultimate award of monetary damages will suffice. *Montgomery v. Carr,* 848 F. Supp. 770 (S.D. Ohio 1993). However, money damages are only adequate if they can be reasonably computed and collected. Plaintiff has demonstrated that defendants' intrusions into their computer systems harm plaintiff's business reputation and goodwill. This is the sort of injury that warrants the issuance of a preliminary injunction because the actual loss is impossible to compute. *Basicomputer Corp. v. Scott,* 973 F.2d 507 (6th Cir. 1992); *Economou v. Physician's Weight Loss Centers of America,* 756 F. Supp. 1024 (N.D. Ohio 1991).

Plaintiff has shown that it will suffer irreparable harm without the grant of the preliminary injunction.

It is improbable that granting the injunction will cause substantial harm to defendant. Even with the grant of this injunction, defendants are free to disseminate their advertisements in other ways not constituting trespass to plaintiff's computer equipment. Further, defendants may continue to send electronic mail messages to the tens of millions of Internet users who are not connected through CompuServe's computer systems.

Finally, the public interest is advanced by the Court's protection of the common law rights of individuals and entities to their personal property. Defendants raise First Amendment concerns and argue that an injunction will adversely impact the public interest. High volumes of junk e-mail devour computer and storage capacity, slow down data transfer between computers over the Internet by congesting the electronic paths through which the messages travel, and cause recipients to spend time and money wading through messages that they do not want. It is ironic that if defendants were to prevail on their First Amendment arguments, the viability of electronic mail as an effective means communication for the rest of society would be put at risk. In light of the foregoing discussion, those arguments are without merit. Further, those subscribing to CompuServe are not injured by the issuance of this injunction. Plaintiff has made a business decision to forbid Cyber Promotions and Mr. Wallace from using its computers to transmit messages to CompuServe subscribers. If CompuServe subscribers are unhappy with that decision, then they may make that known, perhaps by terminating their accounts and transferring to an Internet service provider which accepts unsolicited e-mail advertisements. That is a business risk which plaintiff had assumed.

Having considered the relevant factors, this Court concludes that the preliminary injunction that plaintiff requests is appropriate.

V.

Based on the foregoing, plaintiff's motion for a preliminary injunction is GRANTED. The temporary restraining order filed on October 24, 1996 by this Court is hereby extended in duration until final judgment is entered in this case. Further, defendants Cyber Promotions, Inc. and its president Sanford Wallace are enjoined from sending any unsolicited advertisements to any electronic mail address maintained by plaintiff CompuServe during the pendency of this action.

IT IS SO ORDERED.

JAMES L. GRAHAM
United States District Judge

DATE: February 3, 1997

1ST CASE of Level 1 printed in FULL format.

HOTMAIL CORPORATION, Plaintiff, vs. VAN MONEY PIE INC.; ALS ENTERPRISES, INC.; LCGM, INC.; CHRISTOPHER MOSS d/b/a THE GENESIS NETWORK, INC.; CLAREMONT HOLDINGS LTD.; CONSUMER CONNECTIONS; PALMER & ASSOCIATES; and FINANCIAL RESEARCH GROUP; and DARLENE SNOW d/b/a VISIONARY WEB CREATIONS and/or d/b/a MAXIMUM IMPACT MARKETING, Defendants.

Case No. C98-20064 JW, C-98 JW PVT ENE

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION

1998 U.S. Dist. LEXIS 10729; 47 U.S.P.Q.2D (BNA) 1020

April 16, 1998, Decided
April 16, 1998, Filed

DISPOSITION: Defendants ALS, LCGM, Moss, Palmer, Financial, and Snow, their officers, agents, co-conspirators, servants, affiliates, employees, parent and subsidiary corporations, attorneys and representatives, and all those in privity or acting in concert with defendants are temporarily and preliminarily enjoined and restrained during the pendency of this action from directly or indirectly: Using any images, designs, logos or marks which copy, imitate or simulate Hotmail's HOTMAIL mark, and/or Hotmail's "hotmail.com" domain name.

CORE TERMS: hotmail, e-mail, spam, com, message, subscriber, advertising, sending, transmitted, dilution, domain, provider, consumer, pornography, 'ginated, designated, falsely, Abuse Act, unfair competition, representation, trespass, knowing, point of origin, transmission, reputation, goodwill, prevail, channels, online, authorization

COUNSEL: [*1] HOSIE, WES, SACKS & BRELSFORD, LLP, JAMES F. BRELSFORD, MICHAEL D. SCOTT, NICOLE A. WONG, Menlo Park, California, Attorneys for Plaintiff Hotmail Corporation.

JUDGES: James Ware, U.S. DISTRICT COURT JUDGE.

OPINIONBY: James Ware

OPINION: ORDER GRANTING PRELIMINARY INJUNCTION

[Docket No. 3]

THIS MATTER was submitted on the papers by the Court on the Motion of plaintiff Hotmail Corporation ("Hotmail") for Preliminary Injunction to enjoin defendants ALS Enterprises, Inc. ("ALS"); LCGM, Inc. ("LCGM"); Christopher Moss d/b/a Genesis Network ("Moss"); Palmer & Associates ("Palmer"); Financial Research Group ("Financial") and Darlene Snow d/b/a Visionary Web Creations and/or d/b/a Maximum Impact Marketing ("Snow") from infringing Hotmail's HOTMAIL trade name and service mark, diluting this mark, engaging in acts of unfair competition, violating the Computer Fraud and Abuse Act, breaching a contract, and violating California law. 15 U.S.C. @@ 1125(a)&(c); 18 U.S.C. @ 1030; Cal. Bus. & Prof. Code @@ 14330, 17200; Cal. Civ. Code @@ 1709-10; and 3420-22. Having reviewed the entire court record pertaining to this Motion,

and having considered the evidence and argument of counsel in support of [*2] Hotmail's Motion, the Court enters the following Findings of Fact and Conclusions of Law:

FINDINGS OF FACT

1. Plaintiff Hotmail is a Silicon Valley company that provides free electronic mail ("e-mail") on the World Wide Web. Hotmail's online services allow its over ten million registered subscribers to exchange e-mail messages over the Internet with any other e-mail user who has an Internet e-mail address throughout the world. Every e-mail sent by a Hotmail subscriber automatically displays a header depicting Hotmail's domain name "hotmail.com" and a footer depicting Hotmail's "signature" at the bottom of the e-mail which reads "Get Your Private, Free Email at http://www.hotmail.com." Every e-mail received by a Hotmail subscriber also automatically displays a header depicting Hotmail's domain name. Thus, plaintiff's HOTMAIL mark -- contained within its domain name and signature -- appears on millions of e-mails transmitted worldwide daily.

2. In or about 1996, Hotmail developed the mark HOTMAIL and obtained the Internet domain name "hotmail.com" which incorporates its mark. Hotmail is the sole and exclusive holder of that domain name.

3. In or about 1996, Hotmail began [*3] using its HOTMAIL mark in various forms and styles, continuously in commerce in association with its online services as a means of identifying and distinguishing Hotmail's online services from those of others. Thus Hotmail's mark has appeared in the headers and footers of e-mail sent from and received by Hotmail subscribers, on Hotmail's homepage and on nearly every page of its Website, on letterhead and envelopes, on business cards, in promotional materials and in press releases.

4. Hotmail has spent approximately $ 10 million marketing, promoting, and distributing its services in association with its HOTMAIL mark. Hotmail does not authorize any other e-mail service provider to use its HOTMAIL mark, or Hotmail's domain name or signature.

5. "Spam" is unsolicited commercial bulk e-mail akin to "junk mail" sent through the postal mail. The transmission of spam is a practice widely condemned in the Internet Community and is of significant concern to Hotmail.

6. Hotmail has invested substantial time and money in efforts to disassociate itself from spam and to protect e-mail users worldwide from receiving spam associated in any way with Hotmail.

7. To become a Hotmail subscriber, [*4] one must agree to abide by a Service Agreement ("Terms of Service") which specifically prohibits subscribers from using Hotmail's services to send unsolicited commercial bulk e-mail or "spam," or to send obscene or pornographic messages. Hotmail can terminate the account of any Hotmail subscriber who violates the Terms of Service.

clickthrough

8. In or about the Fall of 1997, Hotmail learned that defendants were sending "spam" e-mails to thousands of Internet e-mail users, which were intentionally falsified in that they contained return addresses bearing Hotmail account return addresses including Hotmail's domain name and thus its mark, when in fact such messages did not originate from Hotmail or a Hotmail account. Such spam messages advertised pornography, bulk e-mailing software, and "get-rich-quick" schemes,

among other things.

9. In addition, Hotmail learned that defendants had created a number of Hotmail accounts for the specific purpose of facilitating their spamming operations. Such accounts were used to collect responses to defendants' e-mails and "bounced back" messages in what amounted to a "drop box" whose contents were never opened, read or responded to. It was these Hotmail accounts [*5] that were used as return addresses by defendants in lieu of defendants' actual return addresses when defendants sent their spam e-mail.

drop boxes for bounce backs

10. As a result of the falsified return addresses described above, Hotmail was inundated with hundreds of thousands of misdirected responses to defendants' spam, including complaints from Hotmail subscribers regarding the spam and "bounced back" e-mails which had been sent by defendants to nonexistent or incorrect e-mail addresses. This overwhelming number of e-mails took up a substantial amount of Hotmail's finite computer space, threatened to delay and otherwise adversely affect Hotmail's subscribers in sending and receiving e-mail, resulted in significant costs to Hotmail in terms of increased personnel necessary to sort and respond to the misdirected complaints, and damaged Hotmail's reputation and goodwill.

damages from forged headers + drop box

11. In particular, Hotmail discovered a spam e-mail message advertising pornographic material that was sent by ALS. While this spam originated from ALS and was transmitted through an E-mail Provider other than Hotmail, ALS falsely designated a real Hotmail e-mail address as the point of origin. The e-mail address chosen for this purpose was [*6] "geri748@hotmail.com."

12. Hotmail also discovered a number of spam e-mail messages advertising pornographic material that were sent by LCGM. While these spam e-mails originated from LCGM and were transmitted through an E-mail Provider other than Hotmail, LCGM falsely designated a number of real Hotmail e-mail address as the points of origin. The e-mail addresses chosen for this purpose were "becky167@hotmail.com;" "deena54@hotmail.com;" "marisa104@hotmail.com;" "shelly345@hotmail.com;" "sonnie67@hotmail.com;" "ashley113@hotmail.com;" "grace44@hotmail.com;" "jess59@hotmail.com;" "kristina17@hotmail.com;" "nellie24@hotmail.com;" and, "tyrona56@hotmail.com."

13. Hotmail also discovered a spam e-mail message advertising pornographic material that was sent by Moss. While this spam originated from Moss and was transmitted through an E-mail Provider other than Hotmail, Moss falsely designated a real Hotmail e-mail address as the point of origin. The e-mail address chosen for this purpose was "rebeccah19@hotmail.com."

14. Hotmail also discovered a spam e-mail message advertising a cable descrambler kit that was sent by Palmer. While this spam originated from Palmer and was transmitted [*7] through an E-mail Provider other than Hotmail, Palmer falsely designated two real Hotmail e-mail addresses as the points of origin. The e-mail addresses chosen for this purpose were "kelCA@hotmail.com" and "angiCA@hotmail.com."

15. Hotmail also discovered a spam e-mail message advertising a service that matches people seeking cash grants that was sent by Financial. While this spam originated from Financial and was transmitted through an E-mail Provider other than Hotmail, Financial falsely designated a real Hotmail e-mail address as the point of origin. The e-mail address chosen for this purpose was "orderdesk66@

hotmail.com."

16. Hotmail also discovered a number of spam e-mail messages advertising pornography that were sent by Snow. While this spam originated from Snow and was transmitted through an E-mail Provider other than Hotmail, Snow falsely designated several real Hotmail e-mail address as the point of origin. The e-mail addresses chosen for this purpose were "bettyharris123@hotmail.com;" "annharris123@hotmail. com;" "cindyharris123@hotmail.com;" "wilmasimpson@hotmail.com;" "rw3570@hotmail.com;" "rw3560@hotmail.com;" and, "jw2244@hotmail.com."

CONCLUSIONS OF LAW [*8]

Jurisdiction and Venue

17. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. @ 1331. This Court has supplemental jurisdiction over the state law claims under 28 U.S.C. @ 1367. This Court has personal jurisdiction over the defendants ALS, LCGM, Moss, Palmer, Financial, and Snow, who have engaged in business activities in or directed in California.

18. Venue is proper in this district pursuant to 28 U.S.C. @ 1391 because a substantial portion of the events giving rise to the claims pled herein occurred in this judicial district and defendants do business in this judicial district.

Standard For Granting Preliminary Injunction

19. The standard for preliminary injunction relief in trademark infringement cases and related actions is well-settled. Hotmail must show either: (a) a likelihood of success on the merits and the possibility of irreparable injury; or (b) the existence of serious questions going to the merits and the balance of hardships tips in Hotmail's favor. Apple Computer, Inc. v. Formula Int'l, Inc., 725 F.2d 521, 523 (9th Cir. 1984).

Plaintiff's Legal Claims

20. Hotmail seeks preliminary [*9] injunctive relief in this Motion for false designations of origin, federal and state dilution, violation of the Computer Fraud and Abuse Act, state and common law unfair competition, breach of contract, fraud and misrepresentation, and trespass to chattel, pursuant to 15 U.S.C. @@ 1116, 1125(a) & (c); 18 U.S.C. @ 1030; Cal. Bus. & Prof. Code @@ 14330, 17203; and Cal Civ. Code @@ 1709-10.

Plaintiff's Likelihood Of Success On Its Claims

1. Lanham Act / Unfair Comp.

False Designation Of Origin And Unfair Competition

21. The core element of a cause of action for false designation of origin under 15 U.S.C. @ 1125(a) as well as other unfair competition is "likelihood of confusion, i.e., whether the similarity of the marks is likely to confuse customers about the source of the products." E. & J. Gallo Winery v. Gallo Cattle Co., 967 F.2d 1280, 1290 (9th Cir. 1992); Academy of Motion Picture Arts & Sciences v. Creative House Promotions, Inc., 944 F.2d 1446, 1454 (9th Cir. 1991).

22. Courts will consider the following factors, among others, as relevant to a determination of the likelihood of confusion for claims under 15 U.S.C. @ 5(a) and related other unfair competition [*10] claims: (a) strength or weakness of plaintiff's mark; (b) the degree of similarity with defendant's mark; (c) class of goods; (d) marketing channels used; (e) evidence of actual confusion; and (f) intent of the defendant. Americana Trading Inc. v. Russ Berrie & Co., 966 F.2d 1284, 1287 (9th Cir. 1992). However, there is not a mandated test for likelihood of confusion applied by the courts in this Circuit, and the appropriate time for full consideration of all relevant factors is when the merits of the case are tried. Apple Computer, 725 F.2d at 526.

23. The majority of these factors supports a finding that Hotmail is likely to succeed on the merits of its claims that defendants' use of the HOTMAIL mark is likely to cause consumer confusion ~~or mistake as to the origin~~, sponsorship, or approval of defendants' spam e-mails and spam e-mail business, and that there are at least serious questions going to the merits of plaintiff's claims.

24. Plaintiff's mark is strong. The "strength" of a mark depends in part on whether it is arbitrary or fanciful, suggestive, merely descriptive, or generic. Chronicle Pub. Co. v. Chronicle Publications, Inc., 733 F. Supp. 1371, 1375 (N.D. [*11] Cal. 1989). In addition, a company's "extensive advertising, length of time in business, public recognition, and uniqueness" all strengthen its trademarks. Century 21 Real Estate Corp. v. Sandlin, 846 F.2d 1175, 1179 (9th Cir. 1988). While the second part of the mark -- "mail" -- may be suggestive by conveying some aspect of the e-mail process, the mark as a whole is arbitrary and fanciful because it neither describes nor suggests that Hotmail is a provider of electronic mail as a Web-based service on the Internet. Moreover, plaintiff has spent substantial sums of money to advertise and market services in association with the mark and has extensively featured the mark its promotions.

25. Defendants' "mark" is not only confusingly similar to plaintiff's mark, it is identical to it. A comparison of defendants' and plaintiff's uses shows such striking similarity that a jury could not help but find that defendants' use is confusing. Indeed, there has been actual confusion among consumers regarding the marks. This factor alone may be determinative. See E. Remy Martin & Co., S.A. v. Shaw-Ross International Imports, Inc., 756 F.2d 1525, 1529, 1530 (11th Cir. 1985) (it is "well-settled" [*12] that "evidence of actual confusion is not necessary to a finding of likelihood of confusion, although it is the best such evidence;" indeed, "a sufficiently strong showing of likelihood of confusion may by itself constitute a showing of substantial likelihood of prevailing on the merits and/or a substantial threat of irreparable harm"); World Carpets, Inc. v. Dick Littrell's New World Carpets, 438 F.2d 482, 489 (5th Cir. 1971) ("there can be no more positive or substantial proof of likelihood of confusion than proof of actual confusion").

26. The class of goods and services distributed by defendants -- e-mails -- which bear a mark identical to plaintiff's, are the same as the class of goods and services distributed by plaintiff -- e-mails.

27. The marketing channels through which the parties sell their goods and services are the same -- via e-mail over the Internet. Their consumer audience is likewise the same. Moreover, because e-mail is specifically designed for the rapid exchange of information, consumers are unlikely to exercise a great deal of care in distinguishing between marks on e-mails they receive.

28. Defendants' intent further supports possible confusion. Levi [*13] Strauss & Co. v. Blue Bell, 632 F.2d 817, 822 (9th Cir. 1981); Pacific Telesis Group v. International Telesis Communications, 994 F.2d 1364, 1369 (9th Cir. 1993). Here, the evidence supports an inference that defendants intended to emulate plaintiff's trademark, given their knowing falsification of e-mail return addresses, their fraudulent creation of Hotmail mailboxes, as well as their attempts to circumvent plaintiff's efforts to prevent its subscribers from receiving spam.

Dilution 2. Dilution

29. The core elements of a cause of action under the federal dilution statute are plaintiff's ownership of a famous mark and dilution of the distinctive quality of plaintiff's mark, regardless of whether consumers are confused about the parties' goods. 15 U.S.C. @ 1125(c)(1). Under the California dilution statute as well, actual injury or likelihood of confusion need not be shown; plaintiff need only show its business reputation is likely to be injured or the distinctive value of its mark is likely to be diluted. Cal. Bus. & Prof. Code @ 14330; Academy, 944 F.2d at 1457.

30. In determining whether a mark is distinctive and famous so as to support a claim for federal dilution, [*14] the Court has considered the following factors: (a) the degree of inherent or acquired distinctiveness of the mark; (b) the duration and extent of use of the mark in connection with the goods or services with which the mark is used; (c) the duration and extent of advertising and publicity of the mark; (d) the geographical extent of the trading area in which the mark is used; (e) the channels of trade for the goods or services with which the mark is used; (f) the degree of recognition of the mark in the trading areas and channels of trade used by the mark's owner and the person against whom the injunction is sought; and (g) the nature and extent of use of the same or similar marks by third parties. 15 U.S.C. @ 1125(c)(1).

31. Under California's anti-dilution statute, the plaintiff need only show the "likelihood of injury to business reputation or of dilution of the distinctive quality of a mark." Cal. Bus. & Prof. Code @ 14330.

32. Here, the evidence supports a finding that plaintiff will likely prevail on its federal and state dilution claims and that there are at least serious questions going to the merits of these claims. First, there is sufficient evidence to lead to a finding [*15] that plaintiff's trademark is "famous" within the meaning of 15 U.S.C. @ 1125(c)(1) and also that it is entitled to state dilution protection. Plaintiff's mark is distinctive, has been advertised and used extensively both nationally and internationally in connection with plaintiff's services, and has established considerable consumer recognition. Moreover, the use of identical marks by defendants who are sending e-mails to thousands of e-mail users across the country and the world through identical trade channels threatens to dilute the distinctiveness of plaintiff's trademark and threatens to harm plaintiff's business reputation.

Is "Hotmail" famous?

Violation Of Computer Fraud And Abuse Act 3. CFAA

33. The Computer Fraud and Abuse Act prohibits any person from knowingly causing the transmission of information which intentionally causes damage, without authorization, to a protected computer. 18 U.S.C. @ 1030.

34. The evidence supports a finding that plaintiff will likely prevail on its Computer Fraud and Abuse Act claim and that there are at least serious questions going to the merits of this claim in that plaintiff has presented evidence of the following: that defendants knowingly falsified [*16] return e-mail addresses so that they included, in place of the actual sender's return address, a number of Hotmail addresses; that such addresses were tied to Hotmail accounts set up by defendants with the intention of collecting never-to-be-read consumer complaints and "bounced back" e-mails; that defendants knowingly caused this false information to be transmitted to thousands of e-mail recipients; that defendants took this action knowing such recipients would use the "reply to" feature to transmit numerous responses to the fraudulently created Hotmail accounts, knowing thousands of messages would be "bounced back" to Hotmail instead of to defendants, and knowing that numerous recipients of defendants' spam would e-mail complaints to Hotmail; that defendants took such actions knowing the risks caused thereby to Hotmail's computer system and online services, which include risks that Hotmail would be forced to withhold or delay the use of computer services to its legitimate subscribers; that defendants' actions caused damage to Hotmail; and that such actions were done by defendants without Hotmail's authorization.

• civil action under CFAA?
• did sign up fr an acct

Breach Of Contract 4. Breach of TOS

35. The evidence supports a finding that [*17] plaintiff will likely prevail on its breach of contract claim and that there are at least serious questions going to the merits of this claim in that plaintiff has presented evidence of the following: that defendants obtained a number of Hotmail mailboxes and access to Hotmail's services; that in so doing defendants agreed to abide by Hotmail's Terms of Service which prohibit using a Hotmail account for purposes of sending spam and/or pornography; that defendants breached their contract with Hotmail by using Hotmail's services to facilitate sending spam and/or pornography; that Hotmail complied with the conditions of the contract except those from which its performance was excused; and that if defendants are not enjoined they will continue to create such accounts in violation of the Terms of Service.

Fraud And Misrepresentation 5. Fraud / Misrep

36. The cause of action for fraud includes willfully deceiving another with intent to induce him to alter his position to his injury or risk by asserting, as a fact, that which is not true, by one who has no reasonable ground for believing it to be true; or by suppressing a fact, by one who is bound to disclose it, or who gives information of other [*18] facts which are likely to mislead for want of communication of that fact; or by making a promise without any intention of performing it. Civ. Code @@ 1709-10.

37. The evidence supports a finding that plaintiff will likely prevail on its fraud and misrepresentation claim and that there are at least serious questions going to the merits of this claim in that plaintiff has presented evidence of the following: that defendants fraudulently obtained a number of Hotmail accounts, promising to abide by the Terms of Service without any intention of doing so and suppressing the fact that such accounts were created for the purpose of facilitating a spamming operation, and that defendants' fraud and misrepresentation caused Hotmail to allow defendants to create and use Hotmail's accounts to Hotmail's injury. In addition, the evidence supports a finding that defendants' falsification of e-mails to make it appear that such

• entered into contract w/o intending to abide by it??

messages and the responses thereto were authorized to be transmitted via Hotmail's computers and stored on Hotmail's computer system -- when defendants knew that sending such spam was unauthorized by Hotmail -- constitutes fraud and misrepresentation, and that Hotmail relied [*19] on such misrepresentations to allow the e-mails to be transmitted over Hotmail's services and to take up storage space on Hotmail's computers, to Hotmail's injury.

o Fraudulent Fraud

Trespass To Chattel

6. Trespass to chattels

38. "Trespass to chattel...lies where an intentional interference with the possession of personal property has proximately caused injury." Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, 1566 (1996).

39. The evidence supports a finding that plaintiff will likely prevail on its trespass to chattel claim and that there are serious questions going to the merits of this claim in that plaintiff has presented evidence of the following: that the computers, computer networks and computer services that comprise Hotmail's e-mail system are the personal property of Hotmail; that defendants obtained consent to create Hotmail accounts within the limitations set forth in the Terms of Service: no spamming and no pornography; that defendants intentionally trespassed on Hotmail's property by knowingly and without authorization creating Hotmail accounts that were used for purposes exceeding the limits of the Terms of Service; that defendants trespassed on Hotmail's computer space by causing tens of [*20] thousands of misdirected e-mail messages to be transmitted to Hotmail without Hotmail's authorization, thereby filling up Hotmail's computer storage space and threatening to damage Hotmail's ability to service its legitimate customers; and that defendants' acts of trespass have damaged Hotmail in terms of added costs for personnel to sort through and respond to the misdirected e-mails, and in terms of harm to Hotmail's business reputation and goodwill.

exceeding scope of TOS = trespass

Irreparable Harm To Plaintiff

40. In cases where trademark infringement is shown, irreparable harm is presumed. Apple Computer, 725 F.2d at 525; Charles Schwab & Co. v. Hibernia Bank, 665 F. Supp. 800, 812 (N.D. Cal. 1987).

41. Plaintiff has suffered and, if defendants are not enjoined, will continue to suffer irreparable harm from the distribution, promotion and use of e-mails bearing plaintiff's mark -- particularly spam e-mails, some of which advertise pornography -- because of the loss of goodwill and reputation arising from customer confusion about the source of defendants' spam e-mails and/or plaintiff's affiliation or sponsorship of them. This kind of harm is not easily quantified and not adequately compensated [*21] with money damages. Plaintiff thus has no adequate remedy at law.

Balance Of Hardships

42. The Court finds that the irreparable harm to plaintiff should injunctive relief not be granted outweighs any injury to defendants resulting from a temporary injunction. Plaintiff has introduced evidence that it has been involved in extensive distribution and promotion of its online services in association with its mark for years and has expended vast amounts of time and money developing and promoting its mark. Plaintiff also is a service mark owner entitled to avoid having its reputation and goodwill placed in jeopardy. In

contrast, if enjoined, defendants would not suffer harm in that they would be free to continue advertising by means of e-mail so long as they did not use Hotmail's mark or services to facilitate such advertising. Thus, the balance of hardships strongly tips in favor of plaintiff.

Conclusion

43. The Court therefore concludes that plaintiff is entitled to a preliminary injunction on the grounds that plaintiff is likely to succeed on the merits, that there is a possibility of irreparable injury, that there are serious questions going to the merits, [*22] and that the balance of hardships tips sharply in plaintiff's favor. It is therefore,

ORDERED AND ADJUDGED:

Scope of order

That defendants ALS, LCGM, Moss, Palmer, Financial, and Snow, their officers, agents, co-conspirators, servants, affiliates, employees, parent and subsidiary corporations, attorneys and representatives, and all those in privity or acting in concert with defendants are temporarily and preliminarily enjoined and restrained during the pendency of this action from directly or indirectly:

1. Using any images, designs, logos or marks which copy, imitate or simulate Hotmail's HOTMAIL mark, and/or Hotmail's "hotmail.com" domain name for any purpose, including but not limited to any advertisement, promotion, sale or use of any products or services;

• no use of Hotmail marks

2. Performing any action or using any images, designs, logos or marks that are likely to cause confusion, to cause mistake, to deceive, or to otherwise mislead the trade or public into believing that Hotmail and defendants, or any of them, are in any way connected, or that Hotmail sponsors defendants; or that defendants, or any of them, are in any manner affiliated or associated with or under the supervision or control of Hotmail, or that [*23] defendants and Hotmail or Hotmail's services are associated in any way.

• suggesting affiliation

3. Using any images, designs, logos or marks or engaging in any other conduct that creates a likelihood of injury to the business reputation of Hotmail or a likelihood of misappropriation and/or dilution of Hotmail's distinctive mark and the goodwill associated therewith;

• any other injury to rep.

4. Using any trade practices whatsoever, including those complained of herein, which tend to unfairly compete with or injure Hotmail, its business and/or the goodwill appertaining thereto;

• no unfair comp

5. Sending or transmitting, or directing, aiding, or conspiring with others to send or transmit, electronic mail or messages bearing any false, fraudulent, anonymous, inactive, deceptive, or invalid return information, or containing the domain "hotmail.com," or otherwise using any other artifice, scheme or method of transmission that would prevent the automatic return of undeliverable electronic mail to its original and true point of origin or that would cause the e-mail return address to be that of anyone other than the actual sender;

• no forged headers

6. Using, or directing, aiding, or conspiring with others to use, Hotmail's computers or computer networks in any manner [*24] in connection with the transmission or transfer of any form of electronic information across the Internet, including, but not limited to, creating any Hotmail e-mail account,

or becoming a Hotmail subscriber, for purposes other than those permitted by Hotmail's Terms of Services, including but not limited to, for purposes of participating in any way in sending spam e-mail or operating a spamming business, or sending or advertising or promoting pornography and/or sending e-mails for any commercial purpose.

7. Opening, creating, obtaining and/or using, or directing, aiding, or conspiring with others to open, create, obtain and/or use, any Hotmail account or mailbox;

8. Acquiring or compiling Hotmail member addresses for use in the transmission of unsolicited promotional messages to those Hotmail members; and,

9. Sending or transmitting, or directing, aiding, or conspiring with others to send or transmit, any unsolicited electronic mail message, or any electronic communication of any kind, to or through Hotmail or its members without prior written authorization.

IT IS FURTHER ORDERED AND ADJUDGED:

That plaintiff shall provide a bond in the amount of only $ 100.

DATED: April [*25] 16, 1998

James Ware

U.S. DISTRICT COURT JUDGE

The UCLA Online Institute for Cyberspace Law and Policy

The Children's Online Privacy Protection Act

H.R. 4328 - OMNIBUS APPROPRIATIONS BILL

TITLE XIII--CHILDREN'S ONLINE PRIVACY PROTECTION

SEC. 1301. SHORT TITLE.

what constitutes personal info?
· cookies
· IP addresses

This title may be cited as the ``Children's Online Privacy Protection Act of 1998".

SEC. 1302. DEFINITIONS.

In this title:
(1) Child.--The term ``child'' means an individual under the age of 13.
(2) Operator.--The term ``operator"--
(A) means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce--
(i) among the several States or with 1 or more foreign nations;
(ii) in any territory of the United States or in the District of Columbia, or between any such territory and--

(I) another such territory; or
(II) any State or foreign nation; or

(iii) between the District of Columbia and any State, territory, or foreign nation; but
(B) does not include any nonprofit entity that would otherwise be exempt from coverage under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).
(3) Commission.--The term ``Commission" means the Federal Trade Commission.
(4) Disclosure.--The term ``disclosure" means, with respect to personal information--
(A) the release of personal information collected from a child in identifiable form by an operator for any purpose, except where such information is provided to a person other than the operator who provides support for the internal operations of the website and does not disclose or use that information for any other purpose; and
Can disclose to web hosts but not co-branding partners
(B) making personal information collected from a child by a website or online service directed to children or with actual knowledge that such information was collected from a child, publicly available in identifiable form, by any means including by a public posting, through the Internet, or through--
(i) a home page of a website;
(ii) a pen pal service;
(iii) an electronic mail service;
(iv) a message board; or
(v) a chat room.

can't provide community functionality

(5) Federal agency.--The term ``Federal agency" means an agency, as that term is defined in section 551(1) of title 5, United States Code.
(6) Internet.--The term ``Internet" means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or

radio.
(7) Parent.--The term ``parent'' includes a legal guardian.
(8) Personal information.--The term ``personal information'' means individually identifiable information about an individual collected online, including--
(A) a first and last name;
(B) a home or other physical address including street name and name of a city or town;
(C) an e-mail address;
(D) a telephone number;
(E) a Social Security number;
(F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or
(G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.
(9) Verifiable parental consent.--The term ``verifiable parental consent'' means any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.
(10) Website or online service directed to children.--
(A) In general.--The term ``website or online service directed to children'' means--
(i) a commercial website or online service that is targeted to children; or
(ii) that portion of a commercial website or online service that is targeted to children.
(B) Limitation.--A commercial website or online service, or a portion of a commercial website or online service, shall not be deemed directed to children solely for referring or linking to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.
(11) Person.--The term ``person'' means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.
(12) Online contact information.--The term ``online contact information'' means an e-mail address or another substantially similar identifier that permits direct contact with a person online.

SEC. 1303. REGULATION OF UNFAIR AND DECEPTIVE ACTS AND PRACTICES IN CONNECTION WITH THE COLLECTION AND USE OF PERSONAL INFORMATION FROM AND ABOUT CHILDREN ON THE INTERNET.

(a) Acts Prohibited.--
(1) In general.--It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b).
(2) Disclosure to parent protected.--Notwithstanding paragraph (1), neither an operator of such a website or online service nor the operator's agent shall be held to be liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under subsection (b)(1)(B)(iii) to the parent of a child.
(b) Regulations.--
(1) In general.--Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate under section 553 of title 5, United States Code, regulations that--
(A) require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child--
(i) to provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information; and
(ii) to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children;
(B) require the operator to provide, upon request of a parent under this subparagraph whose child has provided personal information to that website or online service, upon proper identification of that parent,

to such parent--
(i) a description of the specific types of personal information collected from the child by that operator;
(ii) the opportunity at any time to refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child; and
(iii) notwithstanding any other provision of law, a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child;
(C) prohibit conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and
(D) require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.
(2) When consent not required.--The regulations shall provide that verifiable parental consent under paragraph
(1)(A)(ii) is not required in the case of--
(A) online contact information collected from a child that is used only to respond directly on a one-time basis to a specific request from the child and is not used to recontact the child and is not maintained in retrievable form by the operator;
(B) a request for the name or online contact information of a parent or child that is used for the sole purpose of obtaining parental consent or providing notice under this section and where such information is not maintained in retrievable form by the operator if parental consent is not obtained after a reasonable time;
(C) online contact information collected from a child that is used only to respond more than once directly to a specific request from the child and is not used to recontact the child beyond the scope of that request--
(i) if, before any additional response after the initial response to the child, the operator uses reasonable efforts to provide a parent notice of the online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or
(ii) without notice to the parent in such circumstances as the Commission may determine are appropriate, taking into consideration the benefits to the child of access to information and services, and risks to the security and privacy of the child, in regulations promulgated under this subsection;
(D) the name of the child and online contact information (to the extent reasonably necessary to protect the safety of a child participant on the site)--
(i) used only for the purpose of protecting such safety; (ii) not used to recontact the child or for any other purpose; and
(iii) not disclosed on the site,
if the operator uses reasonable efforts to provide a parent notice of the name and online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or
(E) the collection, use, or dissemination of such information by the operator of such a website or online service necessary--
(i) to protect the security or integrity of its website;
(ii) to take precautions against liability;
(iii) to respond to judicial process; or
(iv) to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety.
(3) Termination of service.--The regulations shall permit the operator of a website or an online service to terminate service provided to a child whose parent has refused, under the regulations prescribed under paragraph (1)(B)(ii), to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child.
(c) Enforcement.--Subject to sections 1304 and 1306, a violation of a regulation prescribed under subsection (a) shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).
(d) Inconsistent State Law.--No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or

action described in this title that is inconsistent with the treatment of those activities or actions under this section.

SEC. 1304. SAFE HARBORS.

(a) Guidelines.--An operator may satisfy the requirements of regulations issued under section 1303(b) by following a set of self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, approved under subsection (b).
(b) Incentives.--
(1) Self-regulatory incentives.--In prescribing regulations under section 1303, the Commission shall provide incentives for self-regulation by operators to implement the protections afforded children under the regulatory requirements described in subsection (b) of that section.
(2) Deemed compliance.--Such incentives shall include provisions for ensuring that a person will be deemed to be in compliance with the requirements of the regulations under section 1303 if that person complies with guidelines that, after notice and comment, are approved by the Commission upon making a determination that the guidelines meet the requirements of the regulations issued under section 1303.
(3) Expedited response to requests.--The Commission shall act upon requests for safe harbor treatment within 180 days of the filing of the request, and shall set forth in writing its conclusions with regard to such requests.
(c) Appeals.--Final action by the Commission on a request for approval of guidelines, or the failure to act within 180 days on a request for approval of guidelines, submitted under subsection (b) may be appealed to a district court of the United States of appropriate jurisdiction as provided for in section 706 of title 5, United States Code.

SEC. 1305. ACTIONS BY STATES.

(a) In General.--
(1) Civil actions.--In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates any regulation of the Commission prescribed under section 1303(b), the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to--
(A) enjoin that practice;
(B) enforce compliance with the regulation;
(C) obtain damage, restitution, or other compensation on behalf of residents of the State; or
(D) obtain such other relief as the court may consider to be appropriate.
(2) Notice.--
(A) In general.--Before filing an action under paragraph
(1), the attorney general of the State involved shall provide to the Commission--
(i) written notice of that action; and
(ii) a copy of the complaint for that action.
(B) Exemption.--
(i) In general.--Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general determines that it is not feasible to provide the notice described in that subparagraph before the filing of the action.
(ii) Notification.--In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general files the action.
(b) Intervention.--
(1) In general.--On receiving notice under subsection (a)(2), the Commission shall have the right to intervene in the action that is the subject of the notice.
(2) Effect of intervention.--If the Commission intervenes in an action under subsection (a), it shall have the right--
(A) to be heard with respect to any matter that arises in that action; and
(B) to file a petition for appeal.
(3) Amicus curiae.--Upon application to the court, a person whose self-regulatory guidelines have been approved by the Commission and are relied upon as a defense by any defendant to a proceeding under this section may file amicus curiae in that proceeding.

(c) Construction.--For purposes of bringing any civil action under subsection (a), nothing in this title shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to--
(1) conduct investigations;
(2) administer oaths or affirmations; or
(3) compel the attendance of witnesses or the production of documentary and other evidence.
(d) Actions by the Commission.--In any case in which an action is instituted by or on behalf of the Commission for violation of any regulation prescribed under section 1303, no State may, during the pendency of that action, institute an action under subsection (a) against any defendant named in the complaint in that action for violation of that regulation.
(e) Venue; Service of Process.--
(1) Venue.--Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.
(2) Service of process.--In an action brought under subsection (a), process may be served in any district in which the defendant--
(A) is an inhabitant; or
(B) may be found.

SEC. 1306. ADMINISTRATION AND APPLICABILITY OF ACT.

(a) In General.--Except as otherwise provided, this title shall be enforced by the Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.).
(b) Provisions.--Compliance with the requirements imposed under this title shall be enforced under--
(1) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of--
(A) national banks, and Federal branches and Federal agencies of foreign banks, by the Office of the Comptroller of the Currency;
(B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25(a) of the Federal Reserve Act (12 U.S.C. 601 et seq. and 611 et seq.), by the Board; and
(C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System) and insured State branches of foreign banks, by the Board of Directors of the Federal Deposit Insurance Corporation;
(2) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), by the Director of the Office of Thrift Supervision, in the case of a savings association the deposits of which are insured by the Federal Deposit Insurance Corporation;
(3) the Federal Credit Union Act (12 U.S.C. 1751 et seq.) by the National Credit Union Administration Board with respect to any Federal credit union;
(4) part A of subtitle VII of title 49, United States Code, by the Secretary of Transportation with respect to any air carrier or foreign air carrier subject to that part;
(5) the Packers and Stockyards Act, 1921 (7 U.S.C. 181 et seq.) (except as provided in section 406 of that Act (7 U.S.C. 226, 227)), by the Secretary of Agriculture with respect to any activities subject to that Act; and
(6) the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.) by the Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association.
(c) Exercise of Certain Powers.--For the purpose of the exercise by any agency referred to in subsection (a) of its powers under any Act referred to in that subsection, a violation of any requirement imposed under this title shall be deemed to be a violation of a requirement imposed under that Act. In addition to its powers under any provision of law specifically referred to in subsection (a), each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this title, any other authority conferred on it by law.
(d) Actions by the Commission.--The Commission shall prevent any person from violating a rule of the Commission under section 1303 in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act

(15 U.S.C. 41 et seq.) were incorporated into and made a part of this title. Any entity that violates such rule shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act in the same manner, by the same means, and with the same jurisdiction, power, and duties as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of this title.
(e) Effect on Other Laws.--Nothing contained in the Act shall be construed to limit the authority of the Commission under any other provisions of law.

SEC. 1307. REVIEW.

Not later than 5 years after the effective date of the regulations initially issued under section 1303, the Commission shall--
(1) review the implementation of this title, including the effect of the implementation of this title on practices relating to the collection and disclosure of information relating to children, children's ability to obtain access to information of their choice online, and on the availability of websites directed to children; and
(2) prepare and submit to Congress a report on the results of the review under paragraph (1).

SEC. 1308. EFFECTIVE DATE.

Sections 1303(a), 1305, and 1306 of this title take effect on the later of--
(1) the date that is 18 months after the date of enactment of this Act; or
(2) the date on which the Commission rules on the first application filed for safe harbor treatment under section 1304 if the Commission does not rule on the first such application within one year after the date of enactment of this Act, but in no case later than the date that is 30 months after the date of enactment of this Act.

Cooley Godward LLP

Article Reprints

Drafting a Privacy Policy? Beware!

October 1998
by Eric Goldman
(formerly Eric Schlachter)

Privacy policies have recently become the drafting project *du jour* for cyberspace law practitioners. This new wave of enthusiasm can be attributed to at least three recent phenomena.

First, in June, the FTC released a report entitled "Privacy Online: A Report to Congress, proposing congressional regulation of the collection of information from children. The associated din from the press has been deafening.

Second, consumers seem to be increasingly aware and concerned about their lack of control over their online private information. Ironically, "off-line" risks (such as from magazines, charities and companies that request warranty registration cards) may be far higher but get far less press.

Finally, drafting a privacy policy has seemingly never been easier. TRUSTe, an independent non-profit privacy initiative, has established a wizard that allows a website to automatically generate a turnkey privacy policy. The Direct Marketing Association has created a similar tool. Yahoo, Excite and other major sites have also recently launched comprehensive privacy policies which other websites are copying.

Unfortunately, drafting a privacy policy is like navigating a mine field-it can be done, but it requires extreme care. Special attention must be paid both to the substance of the policy and the procedure by which it is deployed. There are at least 8 "gotchas" awaiting every website considering instituting a privacy policy:

Beware Incomplete Due Diligence. Drafting a privacy policy requires a thorough examination of the website's current and expected practices about collecting and using personal data. The engineering, customer service, marketing and legal departments all have relevant practices that need to be considered and reflected in a privacy policy (or, on occasion, corrected!). Unless a comprehensive analysis is done, the announced privacy practices will likely be incomplete or wrong. Further, as discussed below, it is difficult to legally amend the privacy policy, so the due diligence must be done upfront to avoid being legally locked in an inaccurate privacy policy.

Beware One-Way Binding Obligations. For reasons that are not entirely clear, most companies that have announced privacy policies are posting the policy to the website but not trying to use industry-standard practices to form an agreement with users. While there remains some doubt about the enforceability of mandatory clickthrough agreements, it remains the preferred way to *try* to form a user agreement online.

In contrast, to the extent that a privacy policy is not a mandatory clickthrough, it probably will not be treated as an agreement. If the privacy policy is not an agreement, then it probably cannot be enforced against users or act as a successful disclaimer or delimiter of rights. Nevertheless, users probably can enforce the privacy policy against the website, under theories such as fraudulent misrepresentation, unfair or deceptive trade practices, or possibly unilateral contract. Thus, in the situations where the privacy policy is not a mandatory clickthrough, the website is presented with the anomalous situation that the policy is probably not enforceable against users but is enforceable against the website-in other words, it has one-way binding legal effect.

There are possibly situations where the marketing benefits from a one-way privacy policy outweigh the legal perils, but a one-way policy will always be inadequate to the extent that legally binding consent from users is required (such as the ECPA or under the European privacy directive; see below).

Beware Absolute Guarantees. For maximum marketing benefit, websites like to make absolute statements regarding privacy. However, there are at least 3 unavoidable situations that preclude such guarantees.

First, since no security system is perfect, users' privacy can be breached by hackers. For example, in 1995 Kevin Mitnick hacked into Netcom and stole a database containing over 20,000 user credit card numbers. Had Netcom promised that these numbers would never be disclosed to a third party, Netcom would have been in breach of its promise.

Second, rogue or malevolent employees can deliberately disclose personal information.

Third, well-meaning employees can "inadvertently" disclose information, such as has happened at AOL at least twice within the last year. First, an AOL employee, apparently unaware of AOL's privacy policy and certainly in breach of it, disclosed personally identifiable information about a user (Navy officer Timothy McVeigh) to the Navy. McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998). Second, AOL employees have been "conned" into disclosing or changing account passwords without proper authentication, allowing third parties to hijack accounts. Indeed, customer support personnel are notoriously underpaid and inadequately trained, and thus will make mistakes.

These risks create serious problems for a claim such as "we never willfully disclose individually identifiable information about our customers to any third party without first receiving permission." While a security hack probably does not breach this promise, disclosures by rogue employees and clueless/gullible employees could be a breach.

Beware the ECPA. Many websites are or may be subject to the Electronic Communications Privacy Act (the "ECPA"), 18 U.S.C. §§ 2510-2521 and 2701-2710. Generally, the ECPA regulates the interception of private communications and the accessing and disclosure of stored communications and associated transactional information. The ECPA is a complicated and poorly drafted statute, making compliance difficult, and violations can lead to both civil and criminal remedies. Therefore, entities that might be subject to the ECPA usually attempt to contractually waive application of the statute.

While there are no clear rules on how to effectively waive users' ECPA rights, generally the ECPA focuses on users' expectations of privacy. Therefore, a privacy policy that creates or reinforces user expectations of privacy does not mitigate the application of the statute (if anything, it might create a more solid grounds for an ECPA claim). To actually disclaim expectations of privacy, the privacy policy probably must be a clickthrough.

Beware the Kids. To the extent that any trends regarding the protection of user privacy have emerged, we have clearly seen that collection of data from children will be given special attention. In addition to the FTC's call on Congress to regulate this (as mentioned above), there have been at least 2 well-publicized incidents in this area.

First, in 1997, the FTC considered bringing an enforcement action against KidsCom, a children-oriented website that collected information from children. Although the FTC decided not to bring an enforcement action, to avoid the enforcement action, KidsCom made the following changes: (a) it emails parents when children register at the site, providing notice of its collection practices, and it gives parents the option to opt out of aggregated information disclosure to third parties, (b) it does not disclose personally identifiable information to third parties without prior parental approval which has been faxed or sent by regular mail, (c) it discloses to users the purposes for which information is collected, and (d) it distinguishes more explicitly between editorial content and advertising.

More recently, the FTC entered into a consent order with GeoCities regarding GeoCities' collection and use of personal information. The FTC accused GeoCities of disclosing members' personal information to third parties in contravention of its stated practices, of failing to disclose how it would use member information (including information from children), and of implying an affiliation with a children's club operated by a GeoCities "community leader" which led children to believe that they were supplying their personal information to GeoCities and not the leader. To avoid further action, GeoCities agreed to: (a) notify users about GeoCities' information and disclosure practices, (b) provide users the ability to delete their personal information from GeoCities' databases, (c) clearly identify its affiliation with third parties that may collect information or sponsor activities on GeoCities, and (d) obtain parental consent before collecting and using personal information obtained by children under 13.

While children deserve special protection, effectuating this is problematic for at least 2 reasons.

First, it is impractical to segregate children because there are few good ways to authenticate for age. Most sites do little or no authentication of their users generally, and even fewer authenticate for age (except for the pornography-oriented sites, many of whom now have affiliated with a pay adult verification system such as AdultCheck). As the U.S. Supreme Court stated in 1997, while websites can verify age using a credit card number or an adult password, due to expense and hassle such verification was effectively unavailable to a substantial number of websites. American Civil Liberties Union v. Reno, 117 S. Ct. 2329 (1997). Therefore, in other contexts websites have not been forced by the government to authenticate for age, and it is no more reasonable to do so in the privacy context.

However, as part of a registration process, many websites ask members their age. While this information is not authenticated, users who self-report their age as being below 18 presumably should be given special treatment. Because categorizing users imposes extra costs on the website, some websites will probably choose not to ask users their age to avoid putatively knowing about minors on the site.

Second, children are not capable of forming a legally binding contract. Therefore, while a user agreement may contain restrictions on use by children, under contract law this contract is not enforceable against the child. Ironically, most government entities have sought greater website disclosure directed to children, although presumably these same children cannot enter into a contract that would restrict their behavior on the website.

So what should a non-children-oriented website say in its privacy policy? (Compliance procedures for children-oriented websites are beyond the scope of this article). Informing children of a specified age that they must get parental consent before disclosing information has an uncertain legal effect, but it may be enough to satisfy the FTC. Telling children in the user agreement that they are not welcome to use the site at all may be legally more defensible, but if users are not authenticated, this restriction still rings hollow. Indeed, given the current state of technology, there are no ideal solutions to the problems of dealing with children online. Each website should give special consideration to this problem in light of its particular offerings and practices.

Beware the Europeans. Although there are few U.S. privacy laws on the books, the European Union has adopted the Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the "Privacy Directive"). The Privacy Directive, scheduled to take full effect in October 1998, places meaningful restrictions on the collection and use of personal data (not just online, but as collected from all sources) and effectively requires express user consent in most situations before websites can legally collect and use such data. Many U.S. companies have chosen not to try to comply with the Privacy Directive, considering themselves outside the scope of the law. However, any company that has a connection to the European Union (such as a physical presence or substantial business in Europe) must consider the effects of the law and, in most cases, should comply with the law enterprise-wide.

Beware of Amending a Policy. When a privacy policy is a one-way binding document, there is some ambiguity about how to update it in a legally-effective way against all users. For example, if a website wants to embark on a new secondary use of data it collected, it could either: (a) update its privacy policy, but there is no guarantee that any of the subject users will see or know of this update (and, indeed, since there will be users who never return, these users presumably will never see the updated policy), or (b) make secondary use only of data of users who opt-in, which severely restricts the number of applicable users. Signatories of TRUSTe's License Agreement must do the latter.

To try to mitigate this problem, some sites announce that changes to the policy are automatically effective against users under specified circumstances. As discussed above, this is probably not legally binding against users in the one-way binding situation, and it may not comply with TRUSTe's rules either.

If the privacy policy is part of a properly formed agreement with users, then the user agreement can specify procedures for amendments. In some cases, the stated amendment procedure places the burden on users to check a specified URL periodically for changes. It seems entirely possible that courts might deem this procedure unreasonable, in which case the amendments might not be honored by a court. The more prudent course of conduct is to provide notice of amendments to users that is likely to actually be seen (such as by email or through a mandatory clickthrough) and allow users to terminate their relationship if they disagree.

In any respect, if the website is a TRUSTe licensee, as mentioned above the website can only expand its use of personally identifiable information with user consent. Assuming that some users will not consent (either because they say no or because they do not respond), a website faces the prospect of having groups of users whose data must be treated in accordance with the "old rules." This imposes significant costs on the website to track these users and retain multiple data use and disclosure rules. Therefore, before a website promulgates a "restrictive" privacy policy, the website must either ensure that it will never want broader rights or be prepared to incur the costs of having multiple classes of users in the future. Alternatively, a website has significant incentive to initially promulgate a "permissive" privacy policy, since it will be easier to make the policy more restrictive in the future than to make it more permissive.

Beware Contrary Statements on the Website. Whether a privacy policy is done as a one-way binding policy or as a user agreement that is intended to be an integrated agreement, the website should centralize all privacy-related provisions in one place and remove other statements that are sprinkled throughout the website. Contrary statements elsewhere on the site could be express representations that are actionable. This is especially true if the contrary statements are more restrictive than the privacy policy. Therefore, it is a good idea to do a comprehensive scrub of the website when launching a privacy policy and remove or conform all inconsistent statements.

Conclusion. There are great marketing benefits associated with announcing a privacy policy, and the associated consumer goodwill can reinforce a website's relationship with its customers. Further, if collectively the web industry can show sufficient progress towards self-regulation, industry may be able to forestall the imposition of unfavorable regulation.

However, considerable thought and care must be devoted to preparing a privacy policy that does not create enormous liability for the website. Drafters should proceed with caution to ensure that the website meets both its short-term marketing objectives and long-term risk management and business development objectives.

About the author: Eric Goldman (formerly Eric Schlachter) is an attorney practicing cyberspace law with Cooley Godward LLP, Palo Alto, CA. He also is an adjunct professor of Cyberspace Law at Santa Clara University School of Law. Cooley Godward's web page is located at http://www.cooley.com, and Eric's personal home page is located at http://members.theglobe.com/ericgoldman/. Eric can be reached at goldmane@cooley.com.

Cooley Alerts & Handbooks · Article Reprints · Press Releases · Search

Site Map · Disclaimer · Bookmark this Link · Frames Off
Copyright © 1994 - 1998 Cooley Godward LLP. All rights reserved.
COOLEY and COOLEY GODWARD are registered U.S. service marks of Cooley Godward LLP.

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of

GEOCITIES, a corporation.

FILE NO. 9823015

AGREEMENT CONTAINING CONSENT ORDER

The Federal Trade Commission has conducted an investigation of certain acts and practices of GeoCities, a corporation ("proposed respondent"). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between GeoCities, by its duly authorized officer, and counsel for the Federal Trade Commission that:

1. Proposed respondent GeoCities is a California corporation with its principal office or place of business at 1918 Main Street, Suite 300, Santa Monica, California 90405.

2. Proposed respondent admits all the jurisdictional facts set forth in the draft complaint.

3. Proposed respondent waives:

(a) Any further procedural steps;

(b) The requirement that the Commission's decision contain a statement of findings of fact and conclusions of law; and

(c) All rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.

4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of sixty (60) days and information about it publicly released. The Commission thereafter may either withdraw its acceptance of this agreement and so notify proposed respondent, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

5. This agreement is for settlement purposes only and does not constitute an admission by proposed respondent that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.

6. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission's Rules, the Commission may, without further notice to proposed respondent, (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondent's address as stated in this agreement by any means specified in Section 4.4(a) of the Commission's Rules shall constitute service. Proposed respondent waives any right it may

have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or the agreement may be used to vary or contradict the terms of the order.

7. Proposed respondent has read the draft complaint and consent order. It understands that it may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. "Child" or "children" shall mean a person of age twelve (12) or under.

2. "Parents" or "parental" shall mean a legal guardian, including, but not limited to, a biological or adoptive parent.

3. "Personal identifying information" shall include, but is not limited to, first and last name, home or other physical address (*e.g.*, school), e-mail address, telephone number, or any information that identifies a specific individual, or any information which when tied to the above becomes identifiable to a specific individual.

4. "Disclosure" or "disclosed to third party(ies)" shall mean (a) the release of information in personally identifiable form to any other individual, firm, or organization for any purpose or (b) making publicly available such information by any means including, but not limited to, public posting on or through home pages, pen pal services, e-mail services, message boards, or chat rooms.

5. "Clear(ly) and prominent(ly)" shall mean in a type size and location that are not obscured by any distracting elements and are sufficiently noticeable for an ordinary consumer to read and comprehend, and in a typeface that contrasts with the background against which it appears.

6. "Archived" database shall mean respondent's off-site "back-up" computer tapes containing member profile information and GeoCities Web site information.

7. "Electronically verifiable signature" shall mean a digital signature or other electronic means that ensures a valid consent by requiring: (1) authentication (guarantee that the message has come from the person who claims to have sent it); (2) integrity (proof that the message contents have not been altered, deliberately or accidentally, during transmission); and (3) non-repudiation (certainty that the sender of the message cannot later deny sending it).

8. "Express parental consent" shall mean a parent's affirmative agreement that is obtained by any of the following means: (1) a signed statement transmitted by postal mail or facsimile; (2) authorizing a charge to a credit card via a secure server; (3) e-mail accompanied by an electronically verifiable signature; (4) a procedure that is specifically authorized by statute, regulation, or guideline issued by the Commission; or (5) such other procedure that ensures verified parental consent and ensures the identity of the parent, such as the use of a reliable certifying authority.

9. Unless otherwise specified, "respondent" shall mean GeoCities, its successors and assigns and its officers, agents, representatives, and employees.

10. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission

Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with any online collection of personal identifying information from consumers, in or affecting commerce, shall not make any misrepresentation, in any manner, expressly or by implication, about its collection or use of such information from or about consumers, including, but not limited to, what information will be disclosed to third parties and how the information will be used.

II.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with any online collection of personal identifying information from consumers, in or affecting commerce, shall not misrepresent, in any manner, expressly or by implication, the identity of the party collecting any such information or the sponsorship of any activity on its Web site.

III.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the online collection of personal identifying information from children, in or affecting commerce, shall not collect personal identifying information from any child if respondent has actual knowledge that such child does not have his or her parent's permission to provide the information to respondent. Respondent shall not be deemed to have actual knowledge if the child has falsely represented that (s)he is not a child and respondent does not knowingly possess information that such representation is false.

IV.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the online collection of personal identifying information, in or affecting commerce, shall provide clear and prominent notice to consumers, including the parents of children, with respect to respondent's practices with regard to its collection and use of personal identifying information. Such notice shall include, but is not limited to, disclosure of:

A. what information is being collected (*e.g.*, "name," "home address," "e-mail address," "age," "interests");

B. its intended use(s);

C. the third parties to whom it will be disclosed (*e.g.*, "advertisers of consumer products," mailing list companies," "the general public");

D. the consumer's ability to obtain access to or directly access such information and the means by which (s)he may do so;

E. the consumer's ability to remove directly or have the information removed from respondent's databases and the means by which (s)he may do so; and

F. the procedures to delete personal identifying information from respondent's databases and any limitations related to such deletion.

Such notice shall appear on the home page of respondent's Web site(s) and at each location

on the site(s) at which such information is collected.

Provided that, respondent shall not be required to include the notice at the locations at which information is collected if such information is limited to tracking information and the collection of such information is described in the notice required by this Part.

Provided further that, for purposes of this Part, compliance with all of the following shall be deemed adequate notice: (a) placement of a clear and prominent hyperlink or button labeled **PRIVACY NOTICE** on the home page(s), which directly links to the privacy notice screen(s); (b) placement of the information required in this Part clearly and prominently on the privacy notice screen(s), followed on the same screen(s) with a button that must be clicked on to make it disappear; and (c) at each location on the site at which any personal identifying information is collected, placement of a clear and prominent hyperlink on the initial screen on which the collection takes place, which links directly to the privacy notice and which is accompanied by the following statement in bold typeface:

> **NOTICE: We collect personal information on this site. To learn more about how we use your information click here.**

V.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the online collection of personal identifying information from children, in or affecting commerce, shall maintain a procedure by which it obtains express parental consent prior to collecting and using such information.

Provided that, respondent may implement the following screening procedure that shall be deemed to be in compliance with this Part. Respondent shall collect and retain certain personal identifying information from a child, including birth date and the child's and parent's e-mail addresses (hereafter "screening information"), enabling respondent to identify the site visitor as a child and to block the child's attempt to register with respondent without express parental consent. If respondent elects to have the child register with it, respondent shall: (1) give notice to the child to have his/her parent provide express parental consent to register; and/or (2) send a notice to the parent's e-mail address for the purpose of obtaining express parental consent. The notice to the child or parent shall provide instructions for the parent to: (1) go to a specific URL on the Web site to receive information on respondent's practices regarding its collection and use of personal identifying information from children and (2) provide express parental consent for the collection and use of such information. Respondent's collection of screening information shall be by a manner that discourages children from providing personal identifying information in addition to the screening information. All personal identifying information collected from a child shall be held by respondent in a secure manner and shall not be used in any manner other than to effectuate the notice to the child or parent, or to block the child from further attempts to register or otherwise provide personal identifying information to respondent without express parental consent. The personal identifying information collected shall not be disclosed to any third party prior to the receipt of express parental consent. If express parental consent is not received by twenty (20) days after respondent's collection of the information from the child, respondent shall remove all such personal identifying information from its databases, except such screening information necessary to block the child from further attempts to register or otherwise provide personal identifying information to respondent without express parental consent.

VI.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall provide a reasonable means for consumers, including the parents of children, to obtain removal of their or their children's personal identifying information collected and retained

by respondent and/or disclosed to third parties, prior to the date of service of this order, as follows:

A. Respondent shall provide a clear and prominent notice to each consumer over the age of twelve (12) from whom it collected personal identifying information and disclosed that information to CMG Information Services, Inc., describing such consumer's options as stated in Part VI.C and the manner in which (s)he may exercise them.

B. Respondent shall provide a clear and prominent notice to the parent of each child from whom it collected personal identifying information prior to May 20, 1998, describing the parent's options as stated in Part VI.C and the manner in which (s)he may exercise them.

C. Respondent shall provide the notice within thirty (30) days after the date of service of this order by e-mail, postal mail, or facsimile. Notice to the parent of a child may be to the e-mail address of the parent and, if not known by respondent, to the e-mail address of the child. The notice shall include the following information:

1. the information that was collected (*e.g.*, "name," "home address," "e-mail address," "age," "interests"); its use(s) and/or intended use(s); and the third parties to whom it was or will be disclosed (*e.g.*, "advertisers of consumer products," "mailing list companies," "the general public") and with respect to children, that the child's personal identifying information may have been made public through various means, such as by publicly posting on the child's personal home page or disclosure by the child through the use of an e-mail account;

2. the consumer's and childs parents right to obtain access to such information and the means by which (s)he may do so;

3. the consumer's and childs parent's right to have the information removed from respondent's or a third party's databases and the means by which (s)he may do so;

4. a statement that childrens information will not be disclosed to third parties, including public posting, without express parental consent to the disclosure or public posting;

5. the means by which express parental consent may be communicated to the respondent permitting disclosure to third parties of a child's information; and

6. a statement that the failure of a consumer over the age of twelve (12) to request removal of the information from respondent's databases will be deemed as approval to its continued retention and/or disclosure to third parties by respondent.

D. Respondent shall provide to consumers, including the parents of children, a reasonable and secure means to request access to or directly access their or their childrens personal identifying information. Such means may include direct access through password protected personal profile, return e-mail bearing an electronically verifiable signature, postal mail, or facsimile.

E. Respondent shall provide to consumers, including the parents of children, a reasonable means to request removal of their or their childrens personal identifying information from respondent's and/or the applicable third party's databases or an

assurance that such information has been removed. Such means may include e-mail, postal mail, or facsimile.

F. The failure of a consumer over the age of twelve (12) to request the actions specified above within twenty (20) days after his/her receipt of the notice required in Part VI.A shall be deemed to be consent to the information's continued retention and use by respondent and any third party.

G. Respondent shall provide to the parent of a child a reasonable means to communicate express parental consent to the retention and/or disclosure to third parties of his/her child's personal identifying information. Respondent shall not use any such information or disclose it to any third party unless and until it receives express parental consent.

H. If, in response to the notice required in Part VI.A, respondent has received a request by a consumer over the age of twelve (12) that respondent should remove from its databases the consumer's personal identifying information or has not received the express consent of a parent of a child to the continued retention and/or disclosure to third parties of a child's personal identifying information by respondent within twenty (20) days after the parent's receipt of the notice required in Part VI.B, respondent shall within ten (10) days:

1. Discontinue its retention and/or disclosure to third parties of such information, including but not limited to (a) removing from its databases all such information, (b) removing all personal home pages created by the child, and (c) terminating all e-mail accounts for the child; and

2. Contact all third parties to whom respondent has disclosed the information, requesting that they discontinue using or disclosing that information to other third parties, and remove the information from their databases.

With respect to any consumer over the age of twelve (12) or any parent of a child who has consented to respondent's continued retention and use of personal identifying information pursuant to this Part, such consumer's or parent's continuing right to obtain access to his/her or a child's personal identifying information or removal of such information from respondent's databases shall be as specified in the notice required by Part IV of this order.

I. Within thirty (30) days after the date of service of this order, respondent shall obtain from a responsible official of each third party to whom it has disclosed personal identifying information and from each GeoCities Community Leader a statement stating that (s)he has been advised of the terms of this order and of respondent's obligations under this Part, and that (s)he agrees, upon notification from respondent, to discontinue using or disclosing a consumer's or child's personal identifying information to other third parties and to remove any such information from its databases.

J. As may be permitted by law, respondent shall cease to do business with any third party that fails within thirty (30) days of the date of service of this order to provide the statement set forth in Part VI.I or whom respondent knows or has reason to know has failed at any time to (a) discontinue using or disclosing a child's personal identifying information to other third parties, or (b) remove any such information from their databases. With respect to any GeoCities Community Leader, the respondent shall cease the Community Leader status of any person who fails to provide the statement set forth in Part VI.I or whom respondent knows or has reason to know has failed at

any time to (a) discontinue using or disclosing a child's personal identifying information to other third parties, or (b) remove any such information from their databases.

For purposes of this Part: "third party(ies)" shall mean each GeoCities Community Leader, CMG Information Services, Inc., Surplus Software, Inc. (Surplus Direct/Egghead Computer), Sage Enterprises, Inc. (GeoPlanet/Planetall), Netopia, Inc. (Netopia), and InfoBeat/Mercury Mail (InfoBeat).

VII.

IT IS FURTHER ORDERED that for the purposes of this order, respondent shall not be required to remove personal identifying information from its archived database if such information is retained solely for the purposes of Web site system maintenance, computer file back-up, to block a child's attempt to register with or otherwise provide personal identifying information to respondent without express parental consent, or to respond to requests for such information from law enforcement agencies or pursuant to judicial process. Except as necessary to respond to requests from law enforcement agencies or pursuant to judicial process, respondent shall not disclose to any third party any information retained it its archived database. In any notice required by this order, respondent shall include information, clearly and prominently, about its policies for retaining information in its archived database.

VIII.

IT IS FURTHER ORDERED that for five (5) years after the date of this order, respondent GeoCities, and its successors and assigns, shall place a clear and prominent hyperlink within its privacy statement which states as follows in bold typeface:

NOTICE: Click here for important information about safe surfing from the Federal Trade Commission.

The hyperlink shall directly link to a hyperlink/URL to be provided to respondent by the Commission. The Commission may change the hyperlink/URL upon thirty (30) days prior written notice to respondent.

IX.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall maintain and upon request make available to the Federal Trade Commission for inspection and copying the following:

Record Keeping

A. For five (5) years after the last date of dissemination of a notice required by this order, a print or electronic copy in HTML format of all documents relating to compliance with Parts IV through VIII of this order, including, but not limited to, a sample copy of every information collection form, Web page, screen, or document containing any representation regarding respondent's information collection and use practices, the notice required by Parts IV through VI, any communication to third parties required by Part VI, and every Web page or screen linking to the Federal Trade Commission Web site. Each Web page copy shall be accompanied by the URL of the Web page where the material was posted online. Electronic copies shall include all text and graphics files, audio scripts, and other computer files used in presenting information on the World Wide Web; and

Provided that, after creation of any Web page or screen in compliance with this order, respondent shall not be required to retain a print or electronic copy of any amended Web page or screen to the extent that the amendment does not affect respondent's

compliance obligations under this order.

B. For five (5) years after the last collection of personal identifying information from a child, all materials evidencing the express parental consent given to respondent.

X.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities with respect to the subject matter of this order. Respondent shall deliver this order to current personnel within thirty (30) days after the date of service of this order, and to future personnel within thirty (30) days after the person assumes such position or responsibilities.

XI.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall establish an "information practices training program" for any employee or GeoCities Community Leader engaged in the collection or disclosure to third parties of consumers' personal identifying information. The program shall include training about respondent's privacy policies, information security procedures, and disciplinary procedures for violations of its privacy policies. Respondent shall provide each such current employee and GeoCities Community Leader with information practices training materials within thirty (30) days after the date of service of this order, and each such future employee or GeoCities Community Leader such materials and training within thirty (30) days after (s)he assumes his/her position or responsibilities.

XII.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

XIII.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall, within sixty (60) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which they have complied with this order.

XIV.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a

complaint will not affect the duration of:

A. Any Part in this order that terminates in less than twenty (20) years;

B. This order's application to any respondent that is not named as a defendant in such complaint; and

C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that the respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

Signed this _____ day of _____ 1998.

GEOCITIES

By: _____
DAVID C. BOHNETT
Chairman

_____
BART A. LAZAR
Seyfarth, Shaw, Fairweather & Geraldson
Counsel for Respondent

_____
RONALD L. PLESSER
Piper & Marbury L.L.P.
Counsel for Respondent

_____
MICHAEL F. BROCKMEYER
Piper & Marbury L.L.P.
Counsel for Respondent

_____
TOBY MILGROM LEVIN
Counsel for the Federal Trade Commission

_____
MARTHA K. LANDESBERG
Counsel for the Federal Trade Commission

_____
DEAN C. FORBES
Counsel for the Federal Trade Commission

_____
CAROLINE G. CURTIN
Counsel for the Federal Trade Commission

APPROVED:

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

AMERICAN CIVIL LIBERTIES UNION OF GEORGIA, et al.,
Plaintiffs,

CIVIL ACTION

1:96-cv-2475-MHS

v.

ZELL MILLER, et al.,
Defendants.

ORDER

This action is before the Court on plaintiffs' motion for preliminary injunction and defendants' motion to dismiss. For the reasons stated below, the Court grants plaintiffs' motion and denies defendants' motion.

Factual Background

Plaintiffs bring this action for declaratory and injunctive relief challenging the constitutionality of Act No. 1029, Ga. Laws 1996, p. 1505, codified at O.C.G.A. § 16-9-93.1 ("act" or "statute"). The act makes it a crime for

> any person . . . knowingly to transmit any data through a computer network . . . for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank or point of access to electronic information if such data uses any individual name . . . to falsely identify the person . . .

and for

> any person . . . knowingly to transmit any data through a computer network . . . if such data uses any . . . trade name, registered trademark, logo, legal or official seal, or copyrighted symbol . . . which would falsely state or imply that such person . . . has permission or is legally authorized to use [it] for such purpose when such permission or authorization has not been obtained.

The parties vigorously dispute the scope of the act. Plaintiffs, a group of individuals and organization members who communicate over the internet, interpret it as imposing unconstitutional content-based restrictions on their right to communicate anonymously and pseudonymously over the internet, as well as on their right to use trade names, logos, and other graphics in a manner held to be constitutional in other contexts.

Plaintiffs argue that the act has tremendous implications for internet users, many of whom "falsely identify" themselves on a regular basis for the purpose of communicating about sensitive topics without subjecting themselves to ostracism or embarrassment. Plaintiffs further contend that the trade name and logo restriction frustrates one of the internet's unique features--the "links"(1) that connect web pages on the World Wide Web and enable

users to browse easily from topic to topic through the computer network system. Plaintiffs claim that the act's broad language is further damaging in that it allows for selective prosecution of persons communicating about controversial topics.

Defendants contend that the act prohibits a much narrower class of communications. They interpret it as forbidding only fraudulent transmissions or the appropriation of the identity of another person or entity for some improper purpose. Defendants ask the Court to abstain from exercising jurisdiction in this case in order to give the Georgia Supreme Court an opportunity to definitively interpret the act.

Motion for Preliminary Injunction

In order to prevail on a preliminary injunction motion, plaintiffs must establish 1) a substantial likelihood of success on the merits; 2) a substantial threat of irreparable injury if the injunction is not granted; 3) that the threatened injury to the plaintiffs outweighs the harm an injunction may cause defendants; and 4) that granting the injunction would not disserve the public interest. Teper v. Miller, 82 F.3d 989, 992-93 n.3 (11th Cir. 1996). The Court concludes that plaintiffs have satisfied each of these requirements and are thus entitled to injunctive relief.

1. Likelihood of Success on the Merits(2)

In their motion to dismiss, defendants assert two affirmative defenses which, if persuasive, would make plaintiffs' success on the merits unlikely. First, defendants argue that because plaintiffs have not been prosecuted or threatened with prosecution under the act, no live controversy exists and plaintiffs therefore lack standing to bring this action. The Court concludes, however, that plaintiffs do have standing because "a credible threat of prosecution" exists. Graham v. Butterworth, 5 F.3d 496, 499 (11th Cir. 1993). When plaintiffs filed this action "they intended to engage in arguably protected conduct, which the statute seemed to proscribe." Id. at 499. Furthermore, the rules of standing are relaxed in the first amendment context where "the statute's alleged danger is, in large measure, one of self-censorship; a harm that can be realized even without an actual prosecution." Virginia v. American Booksellers Ass'n, 484 U.S. 383, 384 (1988).

Defendants also ask the Court to abstain from exercising jurisdiction over this case on the grounds that the law is ambiguous and in need of state court interpretation.(3) However, abstention should rarely be invoked in cases involving facial challenges to statutes allegedly violative of the first amendment. Dombrowski v. Pfister, 380 U.S. 479, 489-90 (1965) (holding abstention "inappropriate for cases [where] . . . statutes are justifiably attacked on their face as abridging free expression"). The reluctance to abstain in first amendment cases recognizes that the delay abstention imposes has a further chilling effect on speech. Zwickler v. Koota, 389 U.S. 241, 252 (1967).

The correct inquiry, when asked to abstain in a case involving a facial statutory challenge, is whether the statute is "fairly subject to an interpretation which will render unnecessary or substantially modify the federal constitutional question." City of Houston v. Hill, 482 U.S. 451, 468 (1987). "If the statute is not obviously susceptible of a limiting construction, then even if the statute has never [been] interpreted by a state court tribunal . . . it is the duty of the federal court to exercise its properly invoked jurisdiction." Id. The Court finds, as set forth below, that O.C.G.A. § 16-9-93.1 is not fairly subject to a limiting construction which would obviate its constitutional problems. Moreover, abstention would impose great costs on plaintiffs by further chilling their expression while they wait for an interpretation of the act by the Georgia Supreme Court or by forcing them to risk prosecution if they choose not to wait. Therefore, the Court finds that abstention is inappropriate in this case.

Having addressed defendants' affirmative defenses, the Court concludes that plaintiffs are likely to prevail on the merits of their claim. It appears from the record that plaintiffs are

likely to prove that the statute imposes content-based restrictions which are not narrowly tailored to achieve the state's purported compelling interest. Furthermore, plaintiffs are likely to show that the statute is overbroad and void for vagueness.

First, because "the identity of the speaker is no different from other components of [a] document's contents that the author is free to include or exclude," McIntyre v. Ohio Elections Comm'n, 115 S. Ct. 1511, 1516 (1995), the statute's prohibition of internet transmissions which "falsely identify" the sender constitutes a presumptively invalid content-based restriction. See R.A.V. v. St. Paul, 505 U.S. 377, 382 (1992). The state may impose content-based restrictions only to promote a "compelling state interest" and only through use of "the least restrictive means to further the articulated interest." Sable Communications of California, Inc. v. FCC, 492 U.S. 115, 126 (1989). Thus, in order to overcome the presumption of invalidity, defendants must demonstrate that the statute furthers a compelling state interest and is narrowly tailored to achieve it.

Defendants allege that the statute's purpose is fraud prevention, which the Court agrees is a compelling state interest. However, the statute is not narrowly tailored to achieve that end and instead sweeps innocent, protected speech within its scope. Specifically, by its plain language the criminal prohibition applies regardless of whether a speaker has any intent to deceive or whether deception actually occurs. Therefore, it could apply to a wide range of transmissions which "falsely identify" the sender, but are not "fraudulent" within the specific meaning of the criminal code.

Not narrowly tailored

Defendants respond that the act does not mean what it says and that, instead, a variety of limiting concepts should be engrafted onto it. First, defendants propose to add an element of fraud, or a specific intent requirement of "intent to defraud" or "intent to deceive" to the act.(4) None of these terms or phrases appears in the statute, however, although they are expressly included in other Georgia criminal statutes which require proof of specific intent. See, e.g., O.C.G.A. §§ 10-1-453, 16-9-1(a), 16-9-2, and 16-8-3.

Second, defendants contend that the act applies only to persons who misappropriate the identity of another specific entity or person. Again, there is nothing in the language of the act from which a reasonable person would infer such a requirement, and the General Assembly has specifically included analogous elements when it meant to do so. See O.C.G.A. § 10-1-453.

Third, defendants seek to limit the restriction on use of trade names, marks, and seals by collapsing the act's two clauses--suggesting that "use" of a mark is prohibited only when it would "falsely identify" the user. Without explanation, this construction borrows the "false identification" portion of the first clause and applies it to the second. In addition to not making sense grammatically, the interpretation also imports into the second clause all of the previously discussed interpretive problems with the phrase "falsely identify." (5)

In construing a statute, the Court must "follow the literal language of the statute 'unless it produces contradiction, absurdity or such an inconvenience as to insure that the legislature meant something else.'" Telecom*USA, Inc. v. Collins, 260 Ga. 362, 363 (1990) (citing Department of Trans. v. City of Atlanta, 255 Ga. 124, 137 (1985)). Only if a statute is "readily susceptible to a narrowing construction" may such an interpretation be applied to save a questionable law. American Booksellers Ass'n, 484 U.S. at 397. The words and phrases defendants seek to add to the act appear nowhere in it. Moreover, defendants' attempt to interpret the act is so confusing and contradictory that it could not possibly constitute grounds for rejecting the act's plain language. Even if the Court could impose a limiting construction on the act, defendants' brief provides no real guidance on what that construction should be, but instead offers a variety of very different possible interpretations in hopes that the Court will select one. The Court concludes, therefore, that the act is not readily susceptible to a limiting construction and that its plain language is not narrowly tailored to promote a compelling state interest.

For similar reasons, plaintiffs are likely to succeed on their overbreadth claim because the statute "sweeps protected activity within its proscription." M.S. News Co. v. Casado, 721 F.2d 1281, 1287 (10th Cir. 1983) (citing Erznoznik v. City of Jacksonville, 422 U.S. 205, 212-13 (1975)). In the first amendment context, the overbreadth doctrine, which invalidates overbroad statutes even when some of their applications are valid, United States v. Salerno, 481 U.S. 739, 745 (1987), is based on the recognition that "the very existence of some broadly written laws has the potential to chill the expressive activity of others not before the Court." Forsyth County v. Nationalist Movement, 505 U.S. 123, 129 (1992).

The Court concludes that the statute was not drafted with the precision necessary for laws regulating speech. On its face, the act prohibits such protected speech as the use of false identification to avoid social ostracism, to prevent discrimination and harassment, and to protect privacy, as well as the use of trade names or logos in non-commercial educational speech, news, and commentary -- a prohibition with well-recognized first amendment problems.(6) Therefore, even if the statute could constitutionally be used to prosecute persons who intentionally "falsely identify" themselves in order to deceive or defraud the public, or to persons whose commercial use of trade names and logos creates a substantial likelihood of confusion or the dilution of a famous mark, the statute is nevertheless overbroad because it operates unconstitutionally for a substantial category of the speakers it covers. Village of Schaumburg v. Citizens for a Better Environment, 444 U.S. 620, 634 (1980).

Finally, plaintiffs are likely to succeed on their claim that the statute is unconstitutionally vague. The void-for-vagueness doctrine requires a criminal statute to "define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." Kolender v. Lawson, 461 U.S. 352, 357 (1983). Like the overbreadth doctrine, the policies underlying the vagueness rule apply with special force where the statute at issue restricts speech. ACLU v. Reno, 929 F. Supp. 824, 860 (E.D. Pa. 1996). The Court concludes that plaintiffs are likely to prove that the statute is void for vagueness because it 1) does not give fair notice of the scope of conduct it proscribes; 2) is conducive to arbitrary enforcement; and 3) infringes upon plaintiffs' free expression. See Grayned v. City of Rockford, 408 U.S. 104, 108-09 (1972).

First, the act fails to give fair notice of proscribed conduct to computer network users by failing to define the following terms and phrases: "falsely identify," "use," "falsely imply," and "point of access to electronic information." These undefined terms provide inadequate notice of the scope of proscribed conduct to persons of ordinary intelligence and thus void the act for vagueness.

The statute criminalizes computer transmissions which "falsely identify" the sender, yet fails to state whether or not proof of specific intent to deceive, or proof of actual deception, is required. Plaintiffs' affidavits demonstrate that, although they have no intent to deceive when sending transmissions which may "falsely identify" them and, indeed, have many legitimate and important reasons for concealing their identity, they cannot determine whether or not their conduct violates the act.

Similarly, the portion of the act relating to trade names and logos fails to define or adequately limit the word "use." Other statutes protecting intellectual property expressly limit the definition of "use" to use in a commercial context. See, e.g., 15 U.S.C. § 1125 (federal trademark infringement law); O.C.G.A. § 10-1-440 (b) (1994) (defining "use" within the meaning of Georgia trademark infringement laws); O.C.G.A. § 10-1-450 (1994) (Georgia trademark infringement law). In contrast, the only limiting concept of "use" in the act is that such use must "falsely imply" that permission to use the mark has been obtained. This restriction, which is also undefined and suffers from the same vagueness problems as the term "falsely identify," fails to provide sufficiently specific notice of proscribed conduct.

Finally, the act fails to explain the phrase "any data . . . over the transmission facilities or through the network facilities of a local telephone network for the purpose of . . . exchanging data with . . . a point of access to electronic information." Plaintiffs contend that this phrase could mean that the act applies not only to computer transmissions per se, but also to transmissions by telephone, fax machine, answering machine, voice mail system, pager, or any other electronic device which might be connected to computer network facilities. The act provides no guidance about these potential applications.

Second, the act's vague provisions create a risk of arbitrary and discriminatory enforcement. As plaintiffs point out, not only does the act fail to notify potential defendants of proscribed conduct, but it also fails to notify law enforcement officials of what exactly is prohibited. The act's failure to specifically articulate proscribed conduct affords prosecutors and police officers substantial room for selective prosecution of persons who express minority viewpoints.

Third, the act's vagueness is particularly harmful because it chills protected expression. Plaintiffs' affidavits indicate that they have already altered what they believe to be innocent and legitimate behavior because of their inability to discern what exactly the act proscribes. Without court intervention, this self-censorship will continue until the act is amended, revoked, or definitively interpreted by the state supreme court.

For all of these reasons, the Court concludes that plaintiffs are likely to succeed on their claim that the act is void for vagueness, overbroad, and not narrowly tailored to promote a compelling state interest.

2. Substantial threat of irreparable injury

Plaintiffs have also demonstrated a substantial threat of irreparable injury in the absence of a preliminary injunction. The Supreme Court has held that "[t]he loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury." Elrod v. Burns, 427 U.S. 347, 373 (1976). As described above, the act has already induced self-censorship. The Court concludes, therefore, that failure to enjoin enforcement of the act will force plaintiffs either to continue self-censorship or to risk criminal prosecution. Thus, plaintiffs have demonstrated a substantial threat of irreparable injury unless a preliminary injunction is issued.

3. Balance of hardships

The balance of hardships weighs heavily in plaintiffs' favor. As stated above, plaintiffs will suffer irreparable injury if prosecution under the statute is not enjoined. In contrast, Georgia already has in place many less restrictive means to address fraud and misrepresentation--the interests defendants claim the act at issue promotes. See, e.g., O.C.G.A. § 16-8-3 (1996) (theft by deception); O.C.G.A. § 16-9-93(a)(2) (1996) (computer theft by deception); O.C.G.A. § 10-1-453 (1994) (unauthorized and deceitful use of name or seal of another); O.C.G.A. § 10-1-393 (Supp. 1996) (unfair and deceptive consumer trade practices). Defendants contend that these statutes do not fully reach problematic behavior over the internet, but they fail adequately to explain why. If the act prevents some ill-defined category of fraud or deception not covered by existing laws, defendants do not articulate why they have a compelling interest in preventing that conduct on the internet but have done nothing to prevent the same practices in the print media. Therefore, the Court concludes that plaintiffs face substantially greater harms if the act is allowed to stand than defendants face if its enforcement is enjoined.

4. Promotion of the Public Interest

Finally, for all the reasons set forth above, a preliminary injunction will advance the public

interest. "No long string of citations is necessary to find that the public interest weighs in favor of having access to a free flow of constitutionally protected speech." Reno, 929 F. Supp. at 851.

5. Conclusion

For the foregoing reasons, the Court DENIES defendants' motion to dismiss [#11-1], GRANTS plaintiffs' motion for preliminary injunction [#3-1], and enjoins defendants from enforcing O.C.G.A. § 16-9-93.1 pending a final determination on the merits of plaintiffs' complaint.

IT IS SO ORDERED, this 20th day of June, 1997.

_____

Marvin H. Shoob, Senior Judge

United States District Court
Northern District of Georgia

NOTES

(1) Links are often graphics or logos which, if "clicked on" by the user with a computer mouse, will transport the user to a different web page covering a new topic of information.

(2) In this section of the order, the Court will also address arguments advanced in defendants' motion to dismiss.

(3) Significantly, this argument contradicts defendants' contention that the statute is sufficiently clear to avoid vagueness and overbreadth challenges.

(4) The terms "fraud," "intent to defraud," and "intent to deceive," although used interchangeably by defendants, are not synonymous in the criminal code. See, e.g., United States v. Godwin, 566 F.2d 975, 976 (5th Cir. 1978). Each term requires proof of different elements, and by using the terms interchangeably, defendants fail to explain which of the distinct elements should be applied to the statute.

Also, the word "falsely"--the only term which actually does appear in the statute--is synonymous with none of the above terms defendants seek to add. "Falsely" means merely "wrongly," "incorrectly," or "not truthfully." Webster's Third New Int'l Dictionary 819 (1976).

(5)To further confuse the matter, defendants suggest elsewhere in their brief that the second clause actually does mean what it says and prohibits all uses of marks which would imply permission for that use which has not been obtained. A fair reading of the clause, as written, is that it prohibits the current use of web page links. The linking function requires publishers of web pages to include symbols designating other web pages which may be of interest to a user. This means that an entity or person's seal may appear on hundreds or thousands of other web pages, just for the purpose of enabling the linking system. The appearance of the seal, although completely innocuous, would definitely "imply" to many users that permission for use had been obtained. Defendants have articulated no compelling state interest that would be furthered by restricting the linking function in this way.

(6) Congress acknowledged the first amendment problems with banning non-commercial use of trademarks by limiting the scope of the new Federal Trademark Dilution Act to apply

to commercial use only. See 15 U.S.C. § 1125(c)(4); H.R. No. 104-374 (1995).

INDEX | JOIN | HOME | SEARCH | FEEDBACK

Copyright 1997, The American Civil Liberties Union

The UCLA Online Institute for Cyberspace Law and Policy

The Child Online Protection Act

H.R. 4328 - OMNIBUS APPROPRIATIONS BILL

TITLE XIV--CHILD ONLINE PROTECTION

SEC. 1401. SHORT TITLE.

This title may be cited as the ``Child Online Protection Act".

SEC. 1402. CONGRESSIONAL FINDINGS.

The Congress finds that--
(1) while custody, care, and nurture of the child resides first with the parent, the widespread availability of the Internet presents opportunities for minors to access materials through the World Wide Web in a manner that can frustrate parental supervision or control;
(2) the protection of the physical and psychological well- being of minors by shielding them from materials that are harmful to them is a compelling governmental interest;
(3) to date, while the industry has developed innovative ways to help parents and educators restrict material that is harmful to minors through parental control protections and self-regulation, such efforts have not provided a national solution to the problem of minors accessing harmful material on the World Wide Web;
(4) a prohibition on the distribution of material harmful to minors, combined with legitimate defenses, is currently the most effective and least restrictive means by which to satisfy the compelling government interest; and
(5) notwithstanding the existence of protections that limit the distribution over the World Wide Web of material that is harmful to minors, parents, educators, and industry must continue efforts to find ways to protect children from being exposed to harmful material found on the Internet.

SEC. 1403. REQUIREMENT TO RESTRICT ACCESS BY MINORS TO MATERIALS COMMERCIALLY DISTRIBUTED BY MEANS OF THE WORLD WIDE WEB THAT ARE HARMFUL TO MINORS.

Part I of title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.) is amended by adding at the end the following new section:

``SEC. 231. RESTRICTION OF ACCESS BY MINORS TO MATERIALS COMMERCIALLY DISTRIBUTED BY MEANS OF WORLD WIDE WEB THAT ARE HARMFUL TO MINORS.

``(a) Requirement To Restrict Access.--
``(1) Prohibited conduct.--Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than 6 months, or both.
``(2) Intentional violations.--In addition to the penalties under paragraph (1), whoever intentionally violates such paragraph shall be subject to a fine of not more than $50,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.
``(3) Civil penalty.--In addition to the penalties under paragraphs (1) and (2), whoever violates paragraph (1) shall be subject to a civil penalty of not more than $50,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

both civil & crim remedies

?

``(b) Inapplicability of Carriers and Other Service Providers.--For purposes of subsection (a), a person shall not be considered to make any communication for commercial purposes to the extent that such person is--
``(1) a telecommunications carrier engaged in the provision of a telecommunications service;
``(2) a person engaged in the business of providing an Internet access service;
``(3) a person engaged in the business of providing an Internet information location tool; or
``(4) similarly engaged in the transmission, storage, retrieval, hosting, formatting, or translation (or any combination thereof) of a communication made by another person, without selection or alteration of the content of the communication, except that such person's deletion of a particular communication or material made by another person in a manner consistent with subsection (c) or section 230 shall not constitute such selection or alteration of the content of the communication.
``(c) Affirmative Defense.--
``(1) Defense.--It is an affirmative defense to prosecution under this section that the defendant, in good faith, has restricted access by minors to material that is harmful to minors--
``(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number;
``(B) by accepting a digital certificate that verifies age; or
``(C) by any other reasonable measures that are feasible under available technology.
``(2) Protection for use of defenses.--No cause of action may be brought in any court or administrative agency against any person on account of any activity that is not in violation of any law punishable by criminal or civil penalty, and that the person has taken in good faith to implement a defense authorized under this subsection or otherwise to restrict or prevent the transmission of, or access to, a communication specified in this section.
``(d) Privacy Protection Requirements.--
``(1) Disclosure of information limited.--A person making a communication described in subsection (a)--
``(A) shall not disclose any information collected for the purposes of restricting access to such communications to individuals 17 years of age or older without the prior written or electronic consent of--
``(i) the individual concerned, if the individual is an adult; or
``(ii) the individual's parent or guardian, if the individual is under 17 years of age; and
``(B) shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the person making such communication and the recipient of such communication.
``(2) Exceptions.--A person making a communication described in subsection (a) may disclose such information if the disclosure is--
``(A) necessary to make the communication or conduct a legitimate business activity related to making the communication; or
``(B) made pursuant to a court order authorizing such disclosure.
``(e) Definitions.--For purposes of this subsection, the following definitions shall apply:
``(1) By means of the world wide web.--The term `by means of the World Wide Web' means by placement of material in a computer server-based file archive so that it is publicly accessible, over the Internet, using hypertext transfer protocol or any successor protocol. Not email, not FTP, not Usenet
``(2) Commercial purposes; engaged in the business.--
``(A) Commercial purposes.--A person shall be considered to make a communication for commercial purposes only if such person is engaged in the business of making such communications.
``(B) Engaged in the business.--The term `engaged in the business' means that the person who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labor to such activities, as a regular course of such person's trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person's sole or principal business or source of income). A person may be considered to be engaged in the business of making, by means of the World Wide Web, communications for commercial purposes that include material that is harmful to minors, only if the person knowingly causes the material that is harmful to minors to be posted on the World Wide Web or knowingly solicits such material to be posted on the World Wide Web.
``(3) Internet.--The term `Internet' means the combination of computer facilities and electromagnetic transmission media, and related equipment and software, comprising the interconnected worldwide

network of computer networks that employ the Transmission Control Protocol/Internet Protocol or any successor protocol to transmit information.
``(4) Internet access service.--The term `Internet access service' means a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services.
``(5) Internet information location tool.--The term `Internet information location tool' means a service that refers or links users to an online location on the World Wide Web. Such term includes directories, indices, references, pointers, and hypertext links.
``(6) Material that is harmful to minors.--The term `material that is harmful to minors' means any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that--
``(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;
``(B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and
``(C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.
``(7) Minor.--The term `minor' means any person under 17 years of age.".

SEC. 1404. NOTICE REQUIREMENT.

(a) Notice.--Section 230 of the Communications Act of 1934 (47 U.S.C. 230) is amended--
(1) in subsection (d)(1), by inserting ``or 231" after ``section 223";
(2) by redesignating subsections (d) and (e) as subsections (e) and (f), respectively; and
(3) by inserting after subsection (c) the following new subsection:
``(d) Obligations of Interactive Computer Service.--A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.".
(b) Conforming Amendment.--Section 223(h)(2) of the Communications Act of 1934 (47 U.S.C. 223(h)(2)) is amended by striking ``230(e)(2)" and inserting ``230(f)(2)".

SEC. 1405. STUDY BY COMMISSION ON ONLINE CHILD PROTECTION.

(a) Establishment.--There is hereby established a temporary Commission to be known as the Commission on Online Child Protection (in this section referred to as the ``Commission") for the purpose of conducting a study under this section regarding methods to help reduce access by minors to material that is harmful to minors on the Internet.
(b) Membership.--The Commission shall be composed of 19 members, as follows:
(1) Industry members.--The Commission shall include--
(A) 2 members who are engaged in the business of providing Internet filtering or blocking services or software;
(B) 2 members who are engaged in the business of providing Internet access services;
(C) 2 members who are engaged in the business of providing labeling or ratings services;
(D) 2 members who are engaged in the business of providing Internet portal or search services;
(E) 2 members who are engaged in the business of providing domain name registration services;
(F) 2 members who are academic experts in the field of technology; and
(G) 4 members who are engaged in the business of making content available over the Internet.

Of the members of the Commission by reason of each subparagraph of this paragraph, an equal number shall be appointed by the Speaker of the House of Representatives and by the Majority Leader of the Senate.
(2) Ex officio members.--The Commission shall include the following officials:

Readers are requested to notify the Reporter of Decisions, Supreme Court of the United States, Wash ington, D.C. 20543, of any typographical or other formal errors, in order that corrections may be made before the preliminary print goes to press.

U.S. Supreme Court

No. 96-511

JANET RENO, ATTORNEY GENERAL OF THE UNITED STATES, et al., APPELLANTS v. AMERICAN CIVIL LIBERTIES UNION et al.

on appeal from the united states district court for the eastern district of pennsylvania

[June 26, 1997]

Justice Stevens delivered the opinion of the Court.

At issue is the constitutionality of two statutory provisions enacted to protect minors from "indecent" and "patently offensive" communications on the Internet. Notwithstanding the legitimacy and importance of the congressional goal of protecting children from harmful materials, we agree with the three judge District Court that the statute abridges "the freedom of speech" protected by the First Amendment. 1

The District Court made extensive findings of fact, most of which were based on a detailed stipulation prepared by the parties. See 929 F. Supp. 824, 830-849 (ED Pa. 1996). 2 The findings describe the character and the dimensions of the Internet, the availability ofsexually explicit material in that medium, and the problems confronting age verification for recipients of Internet communications. Because those findings provide the underpinnings for the legal issues, we begin with a summary of the undisputed facts.

The Internet

The Internet is an international network of interconnected computers. It is the outgrowth of what began in 1969 as a military program called "ARPANET," 3 which was designed to enable computers operated by the military, defense contractors, and universities conducting defense related research to communicate with one another by redundant channels even if some portions of the network were damaged in a war. While the ARPANET no longer exists, it provided an example for the development of a number of civilian networks that, eventually linking with each other, now enable tens of millions of people to communicate with one another and to access vast amounts of information from around the world. The Internet is "a unique and wholly new medium of worldwide human communication." 4

The Internet has experienced "extraordinary growth." 5 The number of "host" computers--those that store information and relay communications--increased from about 300 in 1981 to approximately 9,400,000 by the time of the trial in 1996. Roughly 60% of these hosts are located in the United States. About 40 million people used the Internet at the time of trial, a number that is expected to mushroom to 200 million by 1999.

Individuals can obtain access to the Internet frommany different sources, generally hosts themselves or entities with a host affiliation. Most colleges and universities provide access for their students and faculty; many corporations provide their employees with access through an office network; many communities and local libraries provide free access; and an increasing number of storefront "computer coffee shops" provide access for a small hourly fee. Several major national "online services" such as America Online, CompuServe, the Microsoft Network, and Prodigy offer access to their own extensive proprietary networks as well as a link to the much larger resources of the Internet. These commercial online services had almost 12 million individual subscribers at the time of trial.

Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail ("e mail"),

precisely. But, as presently constituted, those most relevant to this case are electronic mail ("e mail"), automatic mailing list services ("mail exploders," sometimes referred to as "listservs"), "newsgroups," "chat rooms," and the "World Wide Web." All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium--known to its users as "cyberspace"--located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.

E mail enables an individual to send an electronic message--generally akin to a note or letter--to another individual or to a group of addressees. The message is generally stored electronically, sometimes waiting for the recipient to check her "mailbox" and sometimes making its receipt known through some type of prompt. A mail exploder is a sort of e mail group. Subscribers can send messages to a common e mail address, which then forwards the message to the group's other subscribers.Newsgroups also serve groups of regular participants, but these postings may be read by others as well. There are thousands of such groups, each serving to foster an exchange of information or opinion on a particular topic running the gamut from, say, the music of Wagner to Balkan politics to AIDS prevention to the Chicago Bulls. About 100,000 new messages are posted every day. In most newsgroups, postings are automatically purged at regular intervals. In addition to posting a message that can be read later, two or more individuals wishing to communicate more immediately can enter a chat room to engage in real time dialogue--in other words, by typing messages to one another that appear almost immediately on the others' computer screens. The District Court found that at any given time "tens of thousands of users are engaging in conversations on a huge range of subjects." 6 It is "no exaggeration to conclude that the content on the Internet is as diverse as human thought." 7

The best known category of communication over the Internet is the World Wide Web, which allows users to search for and retrieve information stored in remote computers, as well as, in some cases, to communicate back to designated sites. In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world. Some of these documents are simply files containing information. However, more elaborate documents, commonly known as Web "pages," are also prevalent. Each has its own address--%rather like a telephone number." 8 Web pages frequently contain information and sometimes allow the viewer to communicate with the page's (or "site's") author. They generally also contain "links" to otherdocuments created by that site's author or to other (generally) related sites. Typically, the links are either blue or underlined text--sometimes images.

Navigating the Web is relatively straightforward. A user may either type the address of a known page or enter one or more keywords into a commercial "search engine" in an effort to locate sites on a subject of interest. A particular Web page may contain the information sought by the "surfer," or, through its links, it may be an avenue to other documents located anywhere on the Internet. Users generally explore a given Web page, or move to another, by clicking a computer "mouse" on one of the page's icons or links. Access to most Web pages is freely available, but some allow access only to those who have purchased the right from a commercial provider. The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.

From the publishers' point of view, it constitutes a vast platform from which to address and hear from a world wide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and individuals. 9 Publishers may either make their material available to the entire pool of Internet users, or confine access to a selected group, such as those willing to pay for the privilege. "No single organization controls any membership in the Web, nor is there any centralized point from which individual Web sites or services can be blocked from the Web." 10

Sexually Explicit Material

Sexually explicit material on the Internet includes text, pictures, and chat and "extends from the modestly titillating to the hardest core." 11 These files are created, named, and posted in the same manner as material that is not sexually explicit, and may be accessed either deliberately or unintentionally during the course of an imprecise search. "Once a provider posts its content on the

Internet, it cannot prevent that content from entering any community." 12 Thus, for example,

> "when the UCR/California Museum of Photography posts to its Web site nudes by Edward Weston and Robert Mapplethorpe to announce that its new exhibit will travel to Baltimore and New York City, those images are available not only in Los Angeles, Baltimore, and New York City, but also in Cincinnati, Mobile, or Beijing--wherever Internet users live. Similarly, the safer sex instructions that Critical Path posts to its Web site, written in street language so that the teenage receiver can understand them, are available not just in Philadelphia, but also in Provo and Prague." 13

Some of the communications over the Internet that originate in foreign countries are also sexually explicit. 14

Though such material is widely available, users seldomencounter such content accidentally. "A document's title or a description of the document will usually appear before the document itself . . . and in many cases the user will receive detailed information about a site's content before he or she need take the step to access the document. Almost all sexually explicit images are preceded by warnings as to the content." 15 For that reason, the "odds are slim" that a user would enter a sexually explicit site by accident. 16 Unlike communications received by radio or television, "the receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial. A child requires some sophistication and some ability to read to retrieve material and thereby to use the Internet unattended." 17

Systems have been developed to help parents control the material that may be available on a home computer with Internet access. A system may either limit a computer's access to an approved list of sources that have been identified as containing no adult material, it may block designated inappropriate sites, or it may attempt to block messages containing identifiable objectionable features. "Although parental control software currently can screen for certain suggestive words or for known sexually explicit sites, it cannot now screen for sexually explicit images." 18 Nevertheless, the evidence indicates that "a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be available." 19 Did this ever happen?

Age Verification

The problem of age verification differs for different uses of the Internet. The District Court categorically determined that there "is no effective way to determine the identity or the age of a user who is accessing material through e mail, mail exploders, newsgroups or chat rooms." 20 The Government offered no evidence that there was a reliable way to screen recipients and participants in such fora for age. Moreover, even if it were technologically feasible to block minors' access to newsgroups and chat rooms containing discussions of art, politics or other subjects that potentially elicit "indecent" or "patently offensive" contributions, it would not be possible to block their access to that material and "still allow them access to the remaining content, even if the overwhelming majority of that content was not indecent." 21

Technology exists by which an operator of a Web site may condition access on the verification of requested information such as a credit card number or an adult password. Credit card verification is only feasible, however, either in connection with a commercial transaction in which the card is used, or by payment to averification agency. Using credit card possession as a surrogate for proof of age would impose costs on non commercial Web sites that would require many of them to shut down. For that reason, at the time of the trial, credit card verification was "effectively unavailable to a substantial number of Internet content providers." Id., at 846 (finding 102). Moreover, the imposition of such a requirement "would completely bar adults who do not have a credit card and lack the resources to obtain one from accessing any blocked material." 22

Commercial pornographic sites that charge their users for access have assigned them passwords as a method of age verification. The record does not contain any evidence concerning the reliability of these

technologies. Even if passwords are effective for commercial purveyors of indecent material, the District Court found that an adult password requirement would impose significant burdens on noncommercial sites, both because they would discourage users from accessing their sites and because the cost of creating and maintaining such screening systems would be "beyond their reach." 23

In sum, the District Court found:

> "Even if credit card verification or adult password verification were implemented, the Government presented no testimony as to how such systems could ensure that the user of the password or credit card is in fact over 18. The burdens imposed by credit card verification and adult password verification systems make them effectively unavailable to a substantial number of Internet content providers." Ibid. (finding 107).

The Telecommunications Act of 1996, Pub. L. 104-104, 110 Stat. 56, was an unusually important legislative enactment. As stated on the first of its 103 pages, its primary purpose was to reduce regulation and encourage "the rapid deployment of new telecommunications technologies." The major components of the statute have nothing to do with the Internet; they were designed to promote competition in the local telephone service market, the multichannel video market, and the market for over the air broadcasting. The Act includes seven Titles, six of which are the product of extensive committee hearings and the subject of discussion in Reports prepared by Committees of the Senate and the House of Representatives. By contrast, Title V--known as the "Communications Decency Act of 1996" (CDA)--contains provisions that were either added in executive committee after the hearings were concluded or as amendments offered during floor debate on the legislation. An amendment offered in the Senate was the source of the two statutory provisions challenged in this case. 24 Theyare informally described as the "indecent transmission" provision and the "patently offensive display" provision. 25

The first, 47 U. S. C. A. §223(a) (Supp. 1997), prohibits the knowing transmission of obscene or indecent messages to any recipient under 18 years of age. It provides in pertinent part:

> "(a) Whoever--
>
> %(1) in interstate or foreign communications--
>
> . . . . .
>
> "(B) by means of a telecommunications device knowingly--
>
> %(i) makes, creates, or solicits, and
>
> %(ii) initiates the transmission of,
>
> %any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;
>
> . . . . .
>
> "(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,
>
> %shall be fined under Title 18, or imprisoned not more than two years, or both."

The second provision, §223(d), prohibits the knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age. It provides:

> "(d) Whoever--
>
> "~~(1) in interstate or foreign communications knowingly--~~

"(1) in interstate or foreign communications knowingly--

"(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

"(B) uses any interactive computer service to display in a manner available to a person under 18 years of age,

%any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive asmeasured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or

"(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity,

%shall be fined under Title 18, or imprisoned not more than two years, or both."

The breadth of these prohibitions is qualified by two affirmative defenses. See §223(e)(5). 26 One covers those who take "good faith, reasonable, effective, and appropriate actions" to restrict access by minors to the prohibited communications. §223(e)(5)(A). The other covers those who restrict access to covered material by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number or code. §223(e)(5)(B).

On February 8, 1996, immediately after the Presidentsigned the statute, 20 plaintiffs 27 filed suit against the Attorney General of the United States and the Department of Justice challenging the constitutionality of §§223(a)(1) and 223(d). A week later, based on his conclusion that the term "indecent" was too vague to provide the basis for a criminal prosecution, District Judge Buckwalter entered a temporary restraining order against enforcement of §223(a)(1)(B)(ii) insofar as it applies to indecent communications. A second suit was then filed by 27 additional plaintiffs, 28 the two cases were consolidated, and a three judge District Court was convened pursuant to §561 of the Act. 29 After an evidentiary hearing, that Court entered a preliminary injunction against enforcement of both of the challenged provisions. Each of the three judges wrote a separate opinion, but their judgment was unanimous.

Chief Judge Sloviter doubted the strength of the Government's interest in regulating "the vast range of online material covered or potentially covered by the CDA," but acknowledged that the interest was "compelling" with respect to some of that material. 929 F. Supp., at 853. She concluded, nonetheless, that the statute "sweeps more broadly than necessary and thereby chills the expression of adults" and that the terms "patently offensive" and "indecent" were "inherently vague." Id., at 854. She also determined that the affirmative defenses were not "technologically or economically feasible for most providers," specifically considering and rejecting an argument that providers could avoid liability by "tagging" their material in a manner that would allow potential readers to screen out unwanted transmissions. Id., at 856. Chief Judge Sloviter also rejected the Government's suggestion that the scope of the statute could be narrowed by construing it to apply only to commercial pornographers. Id., at 854-855.

Judge Buckwalter concluded that the word "indecent" in §223(a)(1)(B) and the terms "patently offensive" and "in context" in §223(d)(1) were so vague that criminal enforcement of either section would violate the "fundamental constitutional principle" of "simple fairness," id., at 861, and the specific protections of the First and Fifth Amendments, id., at 858. He found no statutory basis for the Government's argument that the challenged provisions would be applied only to "pornographic" materials, noting that, unlike obscenity, "indecency has not been defined to exclude works of serious literary, artistic, political or scientific value." Id., at 863. Moreover, the Government's claim that the work must be considered patently offensive "in context" was itself vague because the relevant context might "refer to, among other things, the nature of the communication as a whole, the time of day it was conveyed, the medium used, the identity of the speaker, or whether or not it is accompanied by appropriate warnings." Id., at 864. He believed that the unique nature of the Internet aggravated the

vagueness of the statute. Id., at 865, n. 9.

Judge Dalzell's review of "the special attributes of Internet communication" disclosed by the evidence convinced him that the First Amendment denies Congress the power to regulate the content of protected speech on the Internet. Id., at 867. His opinion explained at length why he believed the Act would abridge significant protected speech, particularly by noncommercial speakers, while "[p]erversely, commercial pornographers would remain relatively unaffected." Id., at 879. He construed our cases as requiring a "medium specific" approach to the analysis of the regulation of mass communication, id., at 873, and concluded that the Internet--as "the most participatory form of mass speech yet developed," id., at 883--is entitled to "the highest protection from governmental intrusion," ibid. 30

The judgment of the District Court enjoins the Government from enforcing the prohibitions in §223(a)(1)(B) insofar as they relate to "indecent" communications, but expressly preserves the Government's right to investigate and prosecute the obscenity or child pornography activities prohibited therein. The injunction against enforcement of §§223(d)(1) and (2) is unqualified because those provisions contain no separate reference to obscenity or child pornography.

The Government appealed under the Act's special review provisions, §561, 110 Stat. 142-143, and we noted probable jurisdiction, see 519 U. S. ___ (1996). In its appeal, the Government argues that the District Court erred in holding that the CDA violated both the First Amendment because it is overbroad and the Fifth Amendment because it is vague. While we discuss the vagueness of the CDA because of its relevance to the First Amendment overbreadth inquiry, we conclude that the judgment should be affirmed without reaching the Fifth Amendment issue. We begin our analysis by reviewing the principal authorities on which the Government relies. Then, after describing the overbreadth of the CDA, we consider the Government's specific contentions, including its submission that we save portions of the statute either by severance or by fashioning judicial limitations on the scope of its coverage.

In arguing for reversal, the Government contends that the CDA is plainly constitutional under three ofour prior decisions: (1) Ginsberg v. New York, 390 U.S. 629 (1968); (2) FCC v. Pacifica Foundation, 438 U.S. 726 (1978); and (3) Renton v. Playtime Theatres, Inc., 475 U.S. 41 (1986). A close look at these cases, however, raises--rather than relieves--doubts concerning the constitutionality of the CDA.

In Ginsberg, we upheld the constitutionality of a New York statute that prohibited selling to minors under 17 years of age material that was considered obscene as to them even if not obscene as to adults. We rejected the defendant's broad submission that "the scope of the constitutional freedom of expression secured to a citizen to read or see material concerned with sex cannot be made to depend on whether the citizen is an adult or a minor." 390 U.S., at 636. In rejecting that contention, we relied not only on the State's independent interest in the well being of its youth, but also on our consistent recognition of the principle that "the parents' claim to authority in their own household to direct the rearing of their children is basic in the structure of our society." 31 In four important respects, the statute upheld in Ginsberg was narrower than the CDA. First, we noted in Ginsberg that "the prohibition against sales to minors does not bar parents who so desire from purchasing the magazines for their children." Id., at 639. Under the CDA, by contrast, neither the parents' consent--nor even their participation--in the communication would avoid the application of the statute. 32 Second, the New York statute applied only to commercial transactions, id., at 647, whereas the CDA contains no such limitation. Third, the New York statute cabined its definition of material that is harmful to minors with the requirement that it be "utterly without redeeming social importance for minors." Id., at 646. The CDA fails to provide us with any definition of the term "indecent" as used in §223(a)(1) and, importantly, omits any requirement that the "patently offensive" material covered by §223(d) lack serious literary, artistic, political, or scientific value. Fourth, the New York statute defined a minor as a person under the age of 17, whereas the CDA, in applying to all those under 18 years, includes an additional year of those nearest majority.

In Pacifica, we upheld a declaratory order of the Federal Communications Commission, holding that the broadcast of a recording of a 12-minute monologue entitled "Filthy Words" that had previously been delivered to a live audience "could have been the subject of administrative sanctions." 438 U.S., at 730 (internal quotations omitted). The Commission had found that the repetitive use of certain words referring to excretory or sexual activities or organs "in an afternoon broadcast when children are in the

audience was patently offensive" and concluded that the monologue was indecent "as broadcast." Id., at 735. The respondent did not quarrel with the finding that the afternoon broadcast was patently offensive, but contended that it was not "indecent" within the meaning of the relevant statutes because it contained no prurient appeal. After rejecting respondent's statutory arguments, we confronted its two constitutional arguments: (1) that the Commission's construction of its authority to ban indecent speech was so broad that its order had to be set aside even if thebroadcast at issue was unprotected; and (2) that since the recording was not obscene, the First Amendment forbade any abridgement of the right to broadcast it on the radio.

In the portion of the lead opinion not joined by Justices Powell and Blackmun, the plurality stated that the First Amendment does not prohibit all governmental regulation that depends on the content of speech. Id., at 742-743. Accordingly, the availability of constitutional protection for a vulgar and offensive monologue that was not obscene depended on the context of the broadcast. Id., at 744-748. Relying on the premise that "of all forms of communication" broadcasting had received the most limited First Amendment protection, id., at 748-749, the Court concluded that the ease with which children may obtain access to broadcasts, "coupled with the concerns recognized in Ginsberg," justified special treatment of indecent broadcasting. Id., at 749-750.

As with the New York statute at issue in Ginsberg, there are significant differences between the order upheld in Pacifica and the CDA. First, the order in Pacifica, issued by an agency that had been regulating radio stations for decades, targeted a specific broadcast that represented a rather dramatic departure from traditional program content in order to designate when--rather than whether--it would be permissible to air such a program in that particular medium. The CDA's broad categorical prohibitions are not limited to particular times and are not dependent on any evaluation by an agency familiar with the unique characteristics of the Internet. Second, unlike the CDA, the Commission's declaratory order was not punitive; we expressly refused to decide whether the indecent broadcast "would justify a criminal prosecution." Id., at 750. Finally, the Commission's order applied to a medium which as a matter of history had "received the most limited First Amendment protection," id., at 748, in large part because warnings could not adequately protect the listener from unexpected program content. The Internet, however, has no comparable history. Moreover, the District Court found that the risk of encountering indecent material by accident is remote because a series of affirmative steps is required to access specific material.

In Renton, we upheld a zoning ordinance that kept adult movie theatres out of residential neighborhoods. The ordinance was aimed, not at the content of the films shown in the theaters, but rather at the "secondary effects"--such as crime and deteriorating property values--that these theaters fostered: " `It is th[e] secondary effect which these zoning ordinances attempt to avoid, not the dissemination of "offensive" speech.' " 475 U.S., at 49 (quoting Young v. American Mini Theatres, Inc., 427 U.S. 50, 71, n. 34 (1976)). According to the Government, the CDA is constitutional because it constitutes a sort of "cyberzoning" on the Internet. But the CDA applies broadly to the entire universe of cyberspace. And the purpose of the CDA is to protect children from the primary effects of "indecent" and "patently offensive" speech, rather than any "secondary" effect of such speech. Thus, the CDA is a content based blanket restriction on speech, and, as such, cannot be "properly analyzed as a form of time, place, and manner regulation." 475 U.S., at 46. See also Boos v. Barry, 485 U.S. 312, 321 (1988) ("Regulations that focus on the direct impact of speech on its audience" are not properly analyzed under Renton); Forsyth County v. Nationalist Movement, 505 U.S. 123, 134 (1992) ("Listeners' reaction to speech is not a content neutral basis for regulation").

These precedents, then, surely do not require us to uphold the CDA and are fully consistent with the application of the most stringent review of its provisions.

In Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546, 557 (1975), we observed that "[e]ach medium of expression . . . may present its own problems." Thus, some of our cases have recognized special justifications for regulation of the broadcast media that are not applicable to other speakers, see Red Lion Broadcasting Co. v. FCC, 395 U.S. 367 (1969); FCC v. Pacifica Foundation, 438 U.S. 726 (1978). In these cases, the Court relied on the history of extensive government regulation of the broadcast medium, see, e.g., Red Lion, 395 U.S., at 399-400; the scarcity of available frequencies at its

inception, see, e.g., Turner Broadcasting System, Inc. v. FCC, 512 U.S. 622, 637-638 (1994); and its "invasive" nature, see Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115, 128 (1989).

Those factors are not present in cyberspace. Neither before nor after the enactment of the CDA have the vast democratic fora of the Internet been subject to the type of government supervision and regulation that has attended the broadcast industry. 33 Moreover, the Internet is not as "invasive" as radio or television. The District Court specifically found that "[c]ommunications over the Internet do not `invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content `by accident.' " 929 F. Supp., at844 (finding 88). It also found that "[a]lmost all sexually explicit images are preceded by warnings as to the content," and cited testimony that " `odds are slim' that a user would come across a sexually explicit sight by accident." Ibid.

We distinguished Pacifica in Sable, 492 U.S., at 128, on just this basis. In Sable, a company engaged in the business of offering sexually oriented prerecorded telephone messages (popularly known as "dial a porn") challenged the constitutionality of an amendment to the Communications Act that imposed a blanket prohibition on indecent as well as obscene interstate commercial telephone messages. We held that the statute was constitutional insofar as it applied to obscene messages but invalid as applied to indecent messages. In attempting to justify the complete ban and criminalization of indecent commercial telephone messages, the Government relied on Pacifica, arguing that the ban was necessary to prevent children from gaining access to such messages. We agreed that "there is a compelling interest in protecting the physical and psychological well being of minors" which extended to shielding them from indecent messages that are not obscene by adult standards, 492 U.S., at 126, but distinguished our "emphatically narrow holding" in Pacifica because it did not involve a complete ban and because it involved a different medium of communication, id., at 127. We explained that "the dial it medium requires the listener to take affirmative steps to receive the communication." Id., at 127-128. "Placing a telephone call," we continued, "is not the same as turning on a radio and being taken by surprise by an indecent message." Id., at 128.

Finally, unlike the conditions that prevailed when Congress first authorized regulation of the broadcast spectrum, the Internet can hardly be considered a "scarce" expressive commodity. It provides relatively unlimited, low cost capacity for communication of allkinds. The Government estimates that "[a]s many as 40 million people use the Internet today, and that figure is expected to grow to 200 million by 1999." 34 This dynamic, multifaceted category of communication includes not only traditional print and news services, but also audio, video, and still images, as well as interactive, real time dialogue. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer. As the District Court found, "the content on the Internet is as diverse as human thought." 929 F. Supp., at 842 (finding 74). We agree with its conclusion that our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.

Regardless of whether the CDA is so vague that it violates the Fifth Amendment, the many ambiguities concerning the scope of its coverage render it problematic for purposes of the First Amendment. For instance, each of the two parts of the CDA uses a different linguistic form. The first uses the word "indecent," 47 U. S. C. A. §223(a) (Supp. 1997), while the second speaks of material that "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs," §223(d). Given the absence of a definition of either term, 35 this difference in language will provokeuncertainty among speakers about how the two standards relate to each other 36 and just what they mean. 37 Could a spe aker confidently assume that a serious discussion about birth control practices, homosexuality, the First Amendment issues raised by the Appendix to our Pacifica opinion, or the consequences of prison rape would not violate the CDA? This uncertainty undermines the likelihood that the CDA has been carefully tailored to the congressional goal of protecting minors from potentially harmful materials.

The vagueness of the CDA is a matter of special concern for two reasons. First, the CDA is a content based regulation of speech. The vagueness of such a regulation raises special First Amendment concerns because of its obvious chilling effect on free speech. See, e.g., Gentile v. State Bar of Nev., 501 U.S.

1030, 1048-1051 (1991). Second, the CDA is a criminal statute. In addition to the opprobrium and stigma of a criminal conviction, the CDA threatens violators with penalties including up to two years in prison for each act of violation. The severity of criminal sanctions may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images. See, e.g., Dombrowski v. Pfister, 380 U.S. 479, 494 (1965). As a practical matter, this increased deterrent effect, coupled with the "risk of discriminatory enforcement" of vague regulations, poses greater First Amendment concerns than those implicated by the civil regulation reviewed in Denver Area Ed. Telecommunications Consortium, Inc. v. FCC, 518 U. S. ___ (1996).

The Government argues that the statute is no more vague than the obscenity standard this Court established in Miller v. California, 413 U.S. 15 (1973). But that is not so. In Miller, this Court reviewed a criminal conviction against a commercial vendor who mailed brochures containing pictures of sexually explicit activities to individuals who had not requested such materials. Id., at 18. Having struggled for some time to establish a definition of obscenity, we set forth in Miller the test for obscenity that controls to this day:

> "(a) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value." Id., at 24 (internal quotation marks and citations omitted).

Because the CDA's "patently offensive" standard (and, we assume arguendo, its synonymous "indecent" standard) is one part of the three prong Miller test, the Government reasons, it cannot be unconstitutionally vague.

Doing violence to Miller

The Government's assertion is incorrect as a matter of fact. The second prong of the Miller test--the purportedly analogous standard--contains a critical requirement that is omitted from the CDA: that the proscribed material be "specifically defined by the applicable state law." This requirement reduces the vagueness inherent in the open ended term "patently offensive" as used in the CDA. Moreover, the Miller definition is limited to "sexual conduct," whereas the CDA extends also to include (1) "excretory activities" as well as (2) "organs" of both a sexual and excretory nature.

The Government's reasoning is also flawed. Just because a definition including three limitations is not vague, it does not follow that one of those limitations, standing by itself, is not vague. 38 Each of Miller's additional two prongs--(1) that, taken as a whole, the material appeal to the "prurient" interest, and (2) that it "lac[k] serious literary, artistic, political, or scientific value"--critically limits the uncertain sweep of the obscenity definition. The second requirement is particularly important because, unlike the "patently offensive" and "prurient interest" criteria, it is not judged by contemporary community standards. See Pope v. Illinois, 481 U.S. 497, 500 (1987). This "societal value" requirement, absent in the CDA, allows appellate courts to impose some limitations and regularity on the definition by setting, as a matter of law, a national floor for socially redeeming value. The Government's contention that courts will be able to give such legal limitations to the CDA's standards is belied by Miller's own rationale for having juries determine whether material is "patently offensive" according to community standards: that such questions are essentially ones of fact. 39

In contrast to Miller and our other previous cases, the CDA thus presents a greater threat of censoring speech that, in fact, falls outside the statute's scope. Given the vague contours of the coverage of the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection. That danger provides further reason for insisting that the statute not be overly broad. The CDA's burden on protected speech cannot be justified if it could be avoided by a more carefully drafted statute.

We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would

be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.

In evaluating the free speech rights of adults, we have made it perfectly clear that "[s]exual expression which is indecent but not obscene is protected by the First Amendment." Sable, 492 U.S., at 126. See also Carey v. Population Services Int'l, 431 U.S. 678, 701 (1977) ("[W]here obscenity is not involved, we have consistentlyheld that the fact that protected speech may be offensive to some does not justify its suppression"). Indeed, Pacifica itself

admonished that "the fact that society may find speech offensive is not a sufficient reason for suppressing it." 438 U.S., at 745.

It is true that we have repeatedly recognized the governmental interest in protecting children from harmful materials. See Ginsberg, 390 U.S., at 639; Pacifica, 438 U.S., at 749. But that interest does not justify an unnecessarily broad suppression of speech addressed to adults. As we have explained, the Government may not "reduc[e] the adult population . . . to . . . only what is fit for children." Denver, 518 U. S., at ___ (slip op., at 29) (internal quotation marks omitted) (quoting Sable, 492 U.S., at 128). 40 "[R]egardless of the strength of the government's interest" in protecting children, "[t]he level of discourse reaching a mailbox simply cannot be limited to that which would be suitable for a sandbox." Bolger v. Youngs Drug Products Corp., 463 U.S. 60, 74-75 (1983).

The District Court was correct to conclude that the CDA effectively resembles the ban on "dial a porn" invalidated in Sable. 929 F. Supp., at 854. In Sable, 492 U.S., at 129, this Court rejected the argument that we should defer to the congressional judgment that nothing less than a total ban would be effective in preventing enterprising youngsters from gaining access to indecent communications. Sable thus made clear that the mere fact that a statutory regulation of speech was enactedfor the important purpose of protecting children from exposure to sexually explicit material does not foreclose inquiry into its validity. 41 As we pointed out last Term, that inquiry embodies an "over arching commitment" to make sure that Congress has designed its statute to accomplish its purpose "without imposing an unnecessarily great restriction on speech." Denver, 518 U. S., at ___ (slip op., at 11).

In arguing that the CDA does not so diminish adult communication, the Government relies on the incorrect factual premise that prohibiting a transmission whenever it is known that one of its recipients is a minor would not interfere with adult to adult communication. The findings of the District Court make clear that this premise is untenable.

Given the size of the potential audience for most messages, in the absence of a viable age verification process, the sender must be charged with knowing that one or more minors will likely view it. Knowledge that, for instance, one or more members of a 100 person chat group will be minor--and therefore that it would be a crime to send the group an indecent message--would surely burden communication among adults. 42

The District Court found that at the time of trial existing technology did not include any effective method for a sender to prevent minors from obtaining access to its communications on the Internet without also denying access to adults. The Court found no effective way to determine the age of a user who is accessing material through e mail, mail exploders, newsgroups, or chat rooms. 929 F. Supp., at 845 (findings 90-94). As a practical matter, the Court also found that it would be prohibitively expensive for noncommercial--as well as some commercial--speakers who have Web sites to verify that their users are adults. Id., at 845-848 (findings 95-116). 43 These limitations must inevitably curtail a significant amount of adult communication on the Internet. By contrast, the District Court found that "[d]espite its limitations, currently available user based software suggests that a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be widely available." Id., at 842 (finding 73) (emphases added).

The breadth of the CDA's coverage is wholly unprecedented. Unlike the regulations upheld in Ginsberg and Pacifica, the scope of the CDA is not limited to commercial speech or commercial entities. Its open ended prohibitions embrace all nonprofit entities and individuals posting indecent messages or

So could a limit on commercial speech by commercial entities be enforceable?

displaying them on their own computers in the presence of minors. The general,undefined terms "indecent" and "patently offensive" cover large amounts of nonpornographic material with serious educational or other value. 44 Moreover, the "community standards" criterion as applied to the Internet means that any communication available to a nation wide audience will be judged by the standards of the community most likely to be offended by the message. 45 The regulated subject matter includes any of the seven "dirty words" used in the Pacifica monologue, the use of which the Government's expert acknowledged could constitute a felony. See Olsen Test., Tr. Vol. V, 53:16-54:10. It may also extend to discussions about prison rape or safe sexual practices, artistic images that include nude subjects, and arguably the card catalogue of the Carnegie Library.

For the purposes of our decision, we need neither accept nor reject the Government's submission that the First Amendment does not forbid a blanket prohibition on all "indecent" and "patently offensive" messages communicated to a 17 year old--no matter how much valuethe message may contain and regardless of parental approval. It is at least clear that the strength of the Government's interest in protecting minors is not equally strong throughout the coverage of this broad statute. Under the CDA, a parent allowing her 17 year old to use the family computer to obtain information on the Internet that she, in her parental judgment, deems appropriate could face a lengthy prison term. See 47 U. S. C. A. §223(a)(2) (Supp. 1997). Similarly, a parent who sent his 17 year old college freshman information on birth control via e mail could be incarcerated even though neither he, his child, nor anyone in their home community, found the material "indecent" or "patently offensive," if the college town's community thought otherwise.

The breadth of this content based restriction of speech imposes an especially heavy burden on the Government to explain why a less restrictive provision would not be as effective as the CDA. It has not done so. The arguments in this Court have referred to possible alternatives such as requiring that indecent material be "tagged" in a way that facilitates parental control of material coming into their homes, making exceptions for messages with artistic or educational value, providing some tolerance for parental choice, and regulating some portions of the Internet--such as commercial web sites--differently than others, such as chat rooms. Particularly in the light of the absence of any detailed findings by the Congress, or even hearings addressing the special problems of the CDA, we are persuaded that the CDA is not narrowly tailored if that requirement has any meaning at all.

In an attempt to curtail the CDA's facial overbreadth, the Government advances three additional arguments for sustaining the Act's affirmative prohibitions: (1) thatthe CDA is constitutional because it leaves open ample "alternative channels" of communication; (2) that the plain meaning of the Act's "knowledge" and "specific person" requirement significantly restricts its permissible applications; and (3) that the Act's prohibitions are "almost always" limited to material lacking redeeming social value.

The Government first contends that, even though the CDA effectively censors discourse on many of the Internet's modalities--such as chat groups, newsgroups, and mail exploders--it is nonetheless constitutional because it provides a "reasonable opportunity" for speakers to engage in the restricted speech on the World Wide Web. Brief for Appellants 39. This argument is unpersuasive because the CDA regulates speech on the basis of its content. A "time, place, and manner" analysis is therefore inapplicable. See Consolidated Edison Co. of N. Y. v. Public Serv. Comm'n of N. Y., 447 U.S. 530, 536 (1980). It is thus immaterial whether such speech would be feasible on the Web (which, as the Government's own expert acknowledged, would cost up to $10,000 if the speaker's interests were not accommodated by an existing Web site, not including costs for database management and age verification). The Government's position is equivalent to arguing that a statute could ban leaflets on certain subjects as long as individuals are free to publish books. In invalidating a number of laws that banned leafletting on the streets regardless of their content--we explained that "one is not to have the exercise of his liberty of expression in appropriate places abridged on the plea that it may be exercised in some other place." Schneider v. State (Town of Irvington), 308 U.S. 147, 163 (1939).

The Government also asserts that the "knowledge" requirement of both §§223(a) and (d), especially when coupled with the "specific child" element found in §223(d), saves the CDA from overbreadth. Because bothsections prohibit the dissemination of indecent messages only to persons known to be under 18, the Government argues, it does not require transmitters to "refrain from communicating

indecent material to adults; they need only refrain from disseminating such materials to persons they know to be under 18." Brief for Appellants 24. This argument ignores the fact that most Internet fora--including chat rooms, newsgroups, mail exploders, and the Web--are open to all comers. The Government's assertion that the knowledge requirement somehow protects the communications of adults is therefore untenable. Even the strongest reading of the "specific person" requirement of §223(d) cannot save the statute. It would confer broad powers of censorship, in the form of a "heckler's veto," upon any opponent of indecent speech who might simply log on and inform the would be discoursers that his 17 year old child--a "specific person . . . under 18 years of age," 47 U. S. C. A. §223(d)(1)(A) (Supp. 1997)--would be present.

Finally, we find no textual support for the Government's submission that material having scientific, educational, or other redeeming social value will necessarily fall outside the CDA's "patently offensive" and "indecent" prohibitions. See also n. 37, supra.

The Government's three remaining arguments focus on the defenses provided in §223(e)(5). 46 First, relying on the "good faith, reasonable, effective, and appropriate actions" provision, the Government suggests that "tagging" provides a defense that saves the constitutionality of the Act. The suggestion assumes that transmitters may encode their indecent communications in a way that would indicate their contents, thus permitting recipients to block their reception with appropriatesoftware. It is the requirement that the good faith action must be "effective" that makes this defense illusory. The Government recognizes that its proposed screening software does not currently exist. Even if it did, there is no way to know whether a potential recipient will actually block the encoded material. Without the impossible knowledge that every guardian in America is screening for the "tag," the transmitter could not reasonably rely on its action to be "effective."

For its second and third arguments concerning defenses--which we can consider together--the Government relies on the latter half of §223(e)(5), which applies when the transmitter has restricted access by requiring use of a verified credit card or adult identification. Such verification is not only technologically available but actually is used by commercial providers of sexually explicit material. These providers, therefore, would be protected by the defense. Under the findings of the District Court, however, it is not economically feasible for most noncommercial speakers to employ such verification. Accordingly, this defense would not significantly narrow the statute's burden on noncommercial speech. Even with respect to the commercial pornographers that would be protected by the defense, the Government failed to adduce any evidence that these verification techniques actually preclude minors from posing as adults. 47 Given that the risk of criminal sanctions "hovers over each content provider, like the proverbial sword of Damocles," 48 the District Court correctly refused to rely on unproven future technology to save the statute. The Government thus failed to prove that theproffered defense would significantly reduce the heavy burden on adult speech produced by the prohibition on offensive displays.

We agree with the District Court's conclusion that the CDA places an unacceptably heavy burden on protected speech, and that the defenses do not constitute the sort of "narrow tailoring" that will save an otherwise patently invalid unconstitutional provision. In Sable, 492 U.S., at 127, we remarked that the speech restriction at issue there amounted to " `burn[ing] the house to roast the pig.' " The CDA, casting a far darker shadow over free speech, threatens to torch a large segment of the Internet community.

At oral argument, the Government relied heavily on its ultimate fall back position: If this Court should conclude that the CDA is insufficiently tailored, it urged, we should save the statute's constitutionality by honoring the severability clause, see 47 U.S.C. § 608 and construing nonseverable terms narrowly. In only one respect is this argument acceptable.

A severability clause requires textual provisions that can be severed. We will follow §608's guidance by leaving constitutional textual elements of the statute intact in the one place where they are, in fact, severable. The "indecency" provision, 47 U. S. C. A. §223(a) (Supp. 1997), applies to "any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent." (Emphasis added.) Appellees do not challenge the application of the statute to obscene speech, which, they acknowledge, can be banned totally because it enjoys no First Amendment protection. See Miller, 413

U.S., at 18. As set forth by the statute, the restriction of "obscene" material enjoys a textual manifestation separate from that for "indecent" material, which we have held unconstitutional. Therefore, we willsever the term "or indecent" from the statute, leaving the rest of §223(a) standing. In no other respect, however, can §223(a) or §223(d) be saved by such a textual surgery.

The Government also draws on an additional, less traditional aspect of the CDA's severability clause, 47 U. S. C., §608, which asks any reviewing court that holds the statute facially unconstitutional not to invalidate the CDA in application to "other persons or circumstances" that might be constitutionally permissible. It further invokes this Court's admonition that, absent "countervailing considerations," a statute should "be declared invalid to the extent it reaches too far, but otherwise left intact." Brockett v. Spokane Arcades, Inc., 472 U.S. 491, 503-504 (1985). There are two flaws in this argument.

First, the statute that grants our jurisdiction for this expedited review, 47 U. S. C. A. §561 (Supp. 1997), limits that jurisdictional grant to actions challenging the CDA "on its face." Consistent with §561, the plaintiffs who brought this suit and the three judge panel that decided it treated it as a facial challenge. We have no authority, in this particular posture, to convert this litigation into an "as applied" challenge. Nor, given the vast array of plaintiffs, the range of their expressive activities, and the vagueness of the statute, would it be practicable to limit our holding to a judicially defined set of specific applications.

Second, one of the "countervailing considerations" mentioned in Brockett is present here. In considering a facial challenge, this Court may impose a limiting construction on a statute only if it is "readily susceptible" to such a construction. Virginia v. American Bookseller's Assn., Inc., 484 U.S. 383, 397 (1988). See also Erznoznik, v. Jacksonville, 422 U.S. 205, 216 (1975) ("readily subject" to narrowing construction). The open ended character of the CDA provides no guidance whatever for limiting its coverage.

This case is therefore unlike those in which we have construed a statute narrowly because the text or other source of congressional intent identified a clear line that this Court could draw. Cf., e.g., Brockett, 472 U.S., at 504-505 (invalidating obscenity statute only to the extent that word "lust" was actually or effectively excised from statute); United States v. Grace, 461 U.S. 171, 180-183 (1983) (invalidating federal statute banning expressive displays only insofar as it extended to public sidewalks when clear line could be drawn between sidewalks and other grounds that comported with congressional purpose of protecting the building, grounds, and people therein). Rather, our decision in United States v. Treasury Employees, 513 U.S. 454, 479, n. 26 (1995), is applicable. In that case, we declined to "dra[w] one or more lines between categories of speech covered by an overly broad statute, when Congress has sent inconsistent signals as to where the new line or lines should be drawn" because doing so "involves a far more serious invasion of the legislative domain." 49 This Court "will not rewrite a . . . law to conform it to constitutional requirements." American Booksellers, 484 U.S., at 397. 50

In this Court, though not in the District Court, the Government asserts that--in addition to its interest in protecting children--its "[e]qually significant" interest in fostering the growth of the Internet provides an independent basis for upholding the constitutionality of the CDA. Brief for Appellants 19. The Government apparently assumes that the unregulated availability of "indecent" and "patently offensive" material on the Internet is driving countless citizens away from the medium because of the risk of exposing themselves or their children to harmful material.

We find this argument singularly unpersuasive. The dramatic expansion of this new marketplace of ideas contradicts the factual basis of this contention. The record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.

For the foregoing reasons, the judgment of the district court is affirmed.

It is so ordered.

U.S. Supreme Court

No. 96-511

JANET RENO, ATTORNEY GENERAL OF THE UNITED STATES, et al., APPELLANTS v. AMERICAN CIVIL LIBERTIES UNION et al.

on appeal from the united states district court for the eastern district of pennsylvania

[June 26, 1997]

Justice O'Connor, with whom The Chief Justice joins, concurring in the judgment in part and dissenting in part.

I write separately to explain why I view the Communications Decency Act of 1996 (CDA) as little more than an attempt by Congress to create "adult zones" on the Internet. Our precedent indicates that the creation of such zones can be constitutionally sound. Despite the soundness of its purpose, however, portions of the CDA are unconstitutional because they stray from the blueprint our prior cases have developed for constructing a "zoning law" that passes constitutional muster.

Appellees bring a facial challenge to three provisions of the CDA. The first, which the Court describes as the "indecency transmission" provision, makes it a crime to knowingly transmit an obscene or indecent message or image to a person the sender knows is under 18 years old. 47 U. S. C. A. §223(a)(1)(B) (May 1996 Supp.). What the Court classifies as a single " `patently offensive display' " provision, see ante, at 11, is in reality two separate provisions. The first of these makes it a crime to knowingly send a patently offensive message or image to a specific person under the age of 18 ("specificperson" provision). §223(d)(1)(A). The second criminalizes the display of patently offensive messages or images "in a[ny] manner available" to minors ("display" provision). §223(d)(1)(B). None of these provisions purports to keep indecent (or patently offensive) material away from adults, who have a First Amendment right to obtain this speech. Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989) ("Sexual expression which is indecent but not obscene is protected by the First Amendment"). Thus, the undeniable purpose of the CDA is to segregate indecent material on the Internet into certain areas that minors cannot access. See S. Conf. Rep. No. 104-230, p. 189 (1996) (CDA imposes "access restrictions . . . to protect minors from exposure to indecent material").

The creation of "adult zones" is by no means a novel concept. States have long denied minors access to certain establishments frequented by adults. 1 Stateshave also denied minors access to speech deemed to be "harmful to minors." 2 The Court has previously sustained such zoning laws, but only if they respect the First Amendment rights of adults and minors. That isto say, a zoning law is valid if (i) it does not unduly restrict adult access to the material; and (ii) minors have no First Amendment right to read or view the banned material. As applied to the Internet as it exists in 1997, the "display" provision and some applications of the "indecency transmission" and "specific person" provisions fail to adhere to the first of these limiting principles by restricting adults' access to protected materials in certain circumstances. Unlike the Court, however, I would invalidate the provisions only in those circumstances.

Our cases make clear that a "zoning" law is valid only if adults are still able to obtain the regulated speech. If they cannot, the law does more than simply keep children away from speech they have no right to obtain--it interferes with the rights of adults to obtain constitutionally protected speech and effectively "reduce[s] the adult population . . . to reading only what is fit for children." Butler v. Michigan, 352 U.S. 380, 383 (1957). The First Amendment does not tolerate such interference. See id., at 383 (striking down a Michigan criminal law banning sale of books--to minors or adults--that contained words or pictures that " `tende[d] to . . . corrup[t] the morals of youth' "); Sable

Communications, supra (invalidating federal law that made it a crime to transmit indecent, but nonobscene, commercial telephone messages to minors and adults); Bolger v. Youngs Drug Products Corp., 463 U.S. 60, 74 (1983) (striking down a federal law prohibiting the mailing of unsolicited advertisements for contraceptives). If the law does not unduly restrict adults' access to constitutionally protected speech, however, it may be valid. In Ginsberg v. New York, 390 U.S. 629, 634 (1968), for example, the Court sustained a New York law that barred store owners from selling pornographic magazinesto minors in part because adults could still buy those magazines.

The Court in Ginsberg concluded that the New York law created a constitutionally adequate adult zone simply because, on its face, it denied access only to minors. The Court did not question--and therefore necessarily assumed--that an adult zone, once created, would succeed in preserving adults' access while denying minors' access to the regulated speech. Before today, there was no reason to question this assumption, for the Court has previously only considered laws that operated in the physical world, a world that with two characteristics that make it possible to create "adult zones": geography and identity. See Lessig, Reading the Constitution in Cyberspace, 45 Emory L. J. 869, 886 (1996). A minor can see an adult dance show only if he enters an establishment that provides such entertainment. And should he attempt to do so, the minor will not be able to conceal completely his identity (or, consequently, his age). Thus, the twin characteristics of geography and identity enable the establishment's proprietor to prevent children from entering the establishment, but to let adults inside.

The electronic world is fundamentally different. Because it is no more than the interconnection of electronic pathways, cyberspace allows speakers and listeners to mask their identities. Cyberspace undeniably reflects some form of geography; chat rooms and Web sites, for example, exist at fixed "locations" on the Internet. Since users can transmit and receive messages on the Internet without revealing anything about their identities or ages, see Lessig, supra, at 901, however, it is not currently possible to exclude persons from accessing certain messages on the basis of their identity.

Cyberspace differs from the physical world in another basic way: Cyberspace is malleable. Thus, it is possible to construct barriers in cyberspace and use them toscreen for identity, making cyberspace more like the physical world and, consequently, more amenable to zoning laws. This transformation of cyberspace is already underway. Lessig, supra, at 888-889. Id., at 887 (cyberspace "is moving . . . from a relatively unzoned place to a universe that is extraordinarily well zoned"). Internet speakers (users who post-material on the Internet) have begun to zone cyberspace itself through the use of "gateway" technology. Such technology requires Internet users to enter information about themselves--perhaps an adult identification number or a credit card number--before they can access certain areas of cyberspace, 929 F. Supp. 824, 845 (ED Pa. 1996), much like a bouncer checks a person's driver's license before admitting him to a nightclub. Internet users who access information have not attempted to zone cyberspace itself, but have tried to limit their own power to access information in cyberspace, much as a parent controls what her children watch on television by installing a lock box. This user based zoning is accomplished through the use of screening software (such as Cyber Patrol or SurfWatch) or browsers with screening capabilities, both of which search addresses and text for keywords that are associated with "adult" sites and, if the user wishes, blocks access to such sites. Id., at 839-842. The Platform for Internet Content Selection (PICS) project is designed to facilitate user based zoning by encouraging Internet speakers to rate the content of their speech using codes recognized by all screening programs. Id., at 838-839.

Despite this progress, the transformation of cyberspace is not complete. Although gateway technology has been available on the World Wide Web for some time now, id., at 845; Shea v. Reno, 930 F. Supp. 916, 933-934 (SDNY 1996), it is not available to all Web speakers, 929 F. Supp., at 845-846, and is just now becoming technologically feasible for chat rooms and USENETnewsgroups, Brief for Federal Parties 37-38. Gateway technology is not ubiquitous in cyberspace, and because without it "there is no means of age verification," cyberspace still remains largely unzoned--and unzoneable. 929 F. Supp., at 846; Shea, supra, at 934. User based zoning is also in its infancy. For it to be effective, (i) an agreed upon code (or "tag") would have to exist; (ii) screening software or browsers with screening capabilities would have to be able to recognize the "tag"; and (iii) those programs would have to be widely available--and widely used--by Internet users. At present, none of these conditions is true. Screening software "is not in wide use today" and "only a handful of browsers have screening capabilities." Shea,

supra, at 945-946. There is, moreover, no agreed upon "tag" for those programs to recognize. 929 F. Supp., at 848; Shea, supra, at 945.

Although the prospects for the eventual zoning of the Internet appear promising, I agree with the Court that we must evaluate the constitutionality of the CDA as it applies to the Internet as it exists today. Ante, at 36. Given the present state of cyberspace, I agree with the Court that the "display" provision cannot pass muster. Until gateway technology is available throughout cyberspace, and it is not in 1997, a speaker cannot be reasonably assured that the speech he displays will reach only adults because it is impossible to confine speech to an "adult zone." Thus, the only way for a speaker to avoid liability under the CDA is to refrain completely from using indecent speech. But this forced silence impinges on the First Amendment right of adults to make and obtain this speech and, for all intents and purposes, "reduce[s] the adult population [on the Internet] to reading only what is fit for children." Butler, 352 U.S., at 383. As a result, the "display" provision cannot withstand scrutiny. Accord, Sable Communications, 492 U.S., at 126-131; Bolger v.Youngs Drug Products Corp., 463 U.S., at 73-75.

The "indecency transmission" and "specific person" provisions present a closer issue, for they are not unconstitutional in all of their applications. As discussed above, the "indecency transmission" provision makes it a crime to transmit knowingly an indecent message to a person the sender knows is under 18 years of age. 47 U. S. C. A. §223(a)(1)(B) (May 1996 Supp.). The "specific person" provision proscribes the same conduct, although it does not as explicitly require the sender to know that the intended recipient of his indecent message is a minor. §223(d)(1)(A). Appellant urges the Court to construe the provision to impose such a knowledge requirement, see Brief for Federal Parties 25-27, and I would do so. See Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Constr. Trades Council, 485 U.S. 568, 575 (1988) ("[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress").

So construed, both provisions are constitutional as applied to a conversation involving only an adult and one or more minors--e.g., when an adult speaker sends an e mail knowing the addressee is a minor, or when an adult and minor converse by themselves or with other minors in a chat room. In this context, these provisions are no different from the law we sustained in Ginsberg. Restricting what the adult may say to the minors in no way restricts the adult's ability to communicate with other adults. He is not prevented from speaking indecently to other adults in a chat room (because there are no other adults participating in the conversation) and he remains free to send indecent e mails to other adults. The relevant universe contains only one adult, and the adult in that universe has the power to refrain from using indecent speech and consequently to keep allsuch speech within the room in an "adult" zone.

The analogy to Ginsberg breaks down, however, when more than one adult is a party to the conversation. If a minor enters a chat room otherwise occupied by adults, the CDA effectively requires the adults in the room to stop using indecent speech. If they did not, they could be prosecuted under the "indecency transmission" and "specific person" provisions for any indecent statements they make to the group, since they would be transmitting an indecent message to specific persons, one of whom is a minor. Accord, ante, at 30. The CDA is therefore akin to a law that makes it a crime for a bookstore owner to sell pornographic magazines to anyone once a minor enters his store. Even assuming such a law might be constitutional in the physical world as a reasonable alternative to excluding minors completely from the store, the absence of any means of excluding minors from chat rooms in cyberspace restricts the rights of adults to engage in indecent speech in those rooms. The "indecency transmission" and "specific person" provisions share this defect.

But these two provisions do not infringe on adults' speech in all situations. And as discussed below, I do not find that the provisions are overbroad in the sense that they restrict minors' access to a substantial amount of speech that minors have the right to read and view. Accordingly, the CDA can be applied constitutionally in some situations. Normally, this fact would require the Court to reject a direct facial challenge. United States v. Salerno, 481 U.S. 739, 745 (1987) ("A facial challenge to a legislative Act [succeeds only if] the challenger . . . establish[es] that no set of circumstances exists under which the Act would be valid"). Appellees' claim arises under the First Amendment, however, and they argue that the CDA is facially invalid because it is "substantially overbroad"--that is, it "sweeps too broadly . . . [and]

penaliz[es] a substantial amount of speech that isconstitutionally protected," Forsyth County v. Nationalist Movement, 505 U.S. 123, 130 (1992). See Brief for Appellees American Library Association et al. 48; Brief for Appellees American Civil Liberties Union et al. 39-41. I agree with the Court that the provisions are overbroad in that they cover any and all communications between adults and minors, regardless of how many adults might be part of the audience to the communication.

This conclusion does not end the matter, however. Where, as here, "the parties challenging the statute are those who desire to engage in protected speech that the overbroad statute purports to punish . . . [t]he statute may forthwith be declared invalid to the extent that it reaches too far, but otherwise left intact." Brockett v. Spokane Arcades, Inc., 472 U.S. 491, 504 (1985). There is no question that Congress intended to prohibit certain communications between one adult and one or more minors. See 47 U. S. C. A. §223(a)(1)(B) (May 1996 Supp.) (punishing "[w]hoever . . . initiates the transmission of [any indecent communication] knowingly that the recipient of the communication is under 18 years of age"); §223(d)(1)(A) (punishing "[w]hoever . . . send[s] to a specific person or persons under 18 years of age [a patently offensive message]"). There is also no question that Congress would have enacted a narrower version of these provisions had it known a broader version would be declared unconstitutional. 47 U.S.C. § 608 ("If . . . the application [of any provision of the CDA] to any person or circumstance is held invalid, . . . the application of such provision to other persons or circumstances shall not be affected thereby"). I would therefore sustain the "indecency transmission" and "specific person" provisions to the extent they apply to the transmission of Internet communications where the party initiating the communication knows that all of the recipients are minors.

Whether the CDA substantially interferes with the First Amendment rights of minors, and thereby runs afoul of the second characteristic of valid zoning laws, presents a closer question. In Ginsberg, the New York law we sustained prohibited the sale to minors of magazines that were "harmful to minors." Under that law, a magazine was "harmful to minors" only if it was obscene as to minors. 390 U.S., at 632-633. Noting that obscene speech is not protected by the First Amendment, Roth v. United States, 354 U.S. 476, 485 (1957), and that New York was constitutionally free to adjust the definition of obscenity for minors, 390 U.S., at 638, the Court concluded that the law did not "invad[e] the area of freedom of expression constitutionally secured to minors." Id., at 637. New York therefore did not infringe upon the First Amendment rights of minors. Cf. Erznoznik v. Jacksonville, 422 U.S. 205, 213 (1975) (striking down city ordinance that banned nudity that was not "obscene even as to minors").

The Court neither "accept[s] nor reject[s]" the argument that the CDA is facially overbroad because it substantially interferes with the First Amendment rights of minors. Ante, at 32. I would reject it. Ginsberg established that minors may constitutionally be denied access to material that is obscene as to minors. As Ginsberg explained, material is obscene as to minors if it (i) is "patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable . . . for minors"; (ii) appeals to the prurient interest of minors; and (iii) is "utterly without redeeming social importance for minors." 390 U.S., at 633. Because the CDA denies minors the right to obtain material that is "patently offensive"--even if it has some redeeming value for minors and even if it does not appeal to their prurient interests--Congress' rejection of the Ginsberg "harmful to minors" standard means thatthe CDA could ban some speech that is "indecent" (i.e., "patently offensive") but that is not obscene as to minors.

I do not deny this possibility, but to prevail in a facial challenge, it is not enough for a plaintiff to show "some" overbreadth. Our cases require a proof of "real" and "substantial" overbreadth, Broadrick v. Oklahoma, 413 U.S. 601, 615 (1973), and appellees have not carried their burden in this case. In my view, the universe of speech constitutionally protected as to minors but banned by the CDA--i.e., the universe of material that is "patently offensive," but which nonetheless has some redeeming value for minors or does not appeal to their prurient interest--is a very small one. Appellees cite no examples of speech falling within this universe and do not attempt to explain why that universe is substantial "in relation to the statute's plainly legitimate sweep." Ibid. That the CDA might deny minors the right to obtain material that has some "value," see ante, at 32-33, is largely beside the point. While discussions about prison rape or nude art, see ibid., may have some redeeming education value for adults, they do not necessarily have any such value for minors, and under Ginsberg, minors only have a First Amendment right to obtain patently offensive material that has "redeeming social importance for

minors," 390 U.S., at 633 (emphasis added). There is also no evidence in the record to support the contention that "many [e] mail transmissions from an adult to a minor are conversations between family members," ante, at 18, n. 32, and no support for the legal proposition that such speech is absolutely immune from regulation. Accordingly, in my view, the CDA does not burden a substantial amount of minors' constitutionally protected speech.

Thus, the constitutionality of the CDA as a zoning law hinges on the extent to which it substantially interferes with the First Amendment rights of adults. Because therights of adults are infringed only by the "display" provision and by the "indecency transmission" and "specific person" provisions as applied to communications involving more than one adult, I would invalidate the CDA only to that extent. Insofar as the "indecency transmission" and "specific person" provisions prohibit the use of indecent speech in communications between an adult and one or more minors, however, they can and should be sustained. The Court reaches a contrary conclusion, and from that holding that I respectfully dissent.

Footnotes

[Footnote 1] "Congress shall make no law . . . abridging the freedom of speech." U. S. Const., Amdt. 1.

[Footnote 2] The Court made 410 findings, including 356 paragraphs of the parties' stipulation and 54 findings based on evidence received in open court. See 929 F. Supp. at 830, n. 9, 842, n. 15.

[Footnote 3] An acronym for the network developed by the Advanced Research Project Agency.

[Footnote 4] Id., at 844 (finding 81).

[Footnote 5] Id., at 831 (finding 3).

[Footnote 6] Id., at 835 (finding 27).

[Footnote 7] Id., at 842 (finding 74).

[Footnote 8] Id., at 836 (finding 36).

[Footnote 9] "Web publishing is simple enough that thousands of individual users and small community organizations are using the Web to publish their own personal `home pages,' the equivalent of individualized newsletters about the person or organization, which are available to everyone on the Web." Id., at 837 (finding 42).

[Footnote 10] Id., at 838 (finding 46).

[Footnote 11] Id., at 844 (finding 82).

[Footnote 12] Ibid. (finding 86).

[Footnote 13] Ibid. (finding 85).

[Footnote 14] Id., at 848 (finding 117).

[Footnote 15] Id., at 844-845 (finding 88).

[Footnote 16] Ibid.

[Footnote 17] Id., at 845 (finding 89).

[Footnote 18] Id., at 842 (finding 72).

[Footnote 19] Ibid. (finding 73).

[Footnote 20] Id., at 845 (finding 90): "An e mail address provides no authoritative information about the addressee, who may use an e mail `alias' or an anonymous remailer. There is also no universal or reliable listing of e mail addresses and corresponding names or telephone numbers, and any such listing would be or rapidly become incomplete. For these reasons, there is no reliable way in many instances for a sender to know if the e mail recipient is an adult or a minor. The difficulty of e mail age verification is compounded for mail exploders such as listservs, which automatically send information to all e mail addresses on a sender's list. Government expert Dr. Olsen agreed that no current technology could give a speaker assurance that only adults were listed in a particular mail exploder's mailing list."

[Footnote 21] Ibid. (finding 93).

[Footnote 22] Id., at 846 (finding 102).

[Footnote 23] Id., at 847 (findings 104-106): "At least some, if not almost all, non commercial organizations, such as the ACLU, Stop Prisoner Rape or Critical Path AIDS Project, regard charging listeners to access their speech as contrary to their goals of making their materials available to a wide audience free of charge. . . . . "There is evidence suggesting that adult users, particularly casual Web browsers, would be discouraged from retrieving information that required use of a credit card or password. Andrew Anker testified that HotWired has received many complaints from its members about HotWired's registration system, which requires only that a member supply a name, e mail address and self created password. There is concern by commercial content providers that age verification requirements would decrease advertising and revenue because advertisers depend on a demonstration that the sites arewidely available and frequently visited."

[Footnote 24] See Exon Amendment No. 1268, 141 Cong. Rec. S8120 (June 9, 1995). See also id., at S8087. This amendment, as revised, became§502 of the Communications Act of 1996, 110 Stat. 133, 47 U. S. C. A. §§223(a)%(e) (Supp. 1997). Some Members of the House of Representatives opposed the Exon Amendment because they thought it "possible for our parents now to child proof the family computer with these products available in the private sector." They also thought the Senate's approach would "involve the Federal Government spending vast sums of money trying to define elusive terms that are going to lead to a flood of legal challenges while our kids are unprotected." These Members offered an amendment intended as a substitute for the Exon Amendment, but instead enacted as an additional section of the Act entitled "Online Family Empowerment." See 110 Stat. 137, 47 U. S. C. A. §230 (Supp. 1997); 141 Cong. Rec. H8468-H8472. No hearings were held on the provisions that became law. See S. Rep. No. 104-23 (1995), p. 9. After the Senate adopted the Exon amendment, however, its Judiciary Committee did conduct a one day hearing on "Cyberporn and Children." In his opening statement at that hearing, Senator Leahy observed: "It really struck me in your opening statement when you mentioned, Mr. Chairman, that it is the first ever hearing, and you are absolutely right. And yet we had a major debate on the floor, passed legislation overwhelmingly on a subject involving the Internet, legislation that could dramatically change--some would say even wreak havoc--on the Internet. The Senate went in willy nilly, passed legislation, and never once had a hearing, never once had a discussion other than an hour or so on the floor." Cyberporn and Children: The Scope of the Problem, The State of the Technology, and the Need for Congressional Action, Hearing on S. 892 before the Senate Committee on the Judiciary, 104th Cong., 1st Sess., 7-8 (1995).

[Footnote 25] Although the Government and the dissent break §223(d)(1) into two separate "patently offensive" and "display" provisions, we follow the convention of both parties below, as well the District Court's order and opinion, in describing §223(d)(1) as one provision.

[Footnote 26] In full, § 223(e)(5) provides: "(5) It is a defense to a prosecution under subsection (a)(1)(B) or (d) of this section, or under subsection (a)(2) of this section with respect to the use of a facility for an activity under subsection (a)(1)(B) of this section that a person-- "(A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate

measures to restrict minors from such communications, including any method which is feasible under available technology; or "(B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number."

[Footnote 27] American Civil Liberties Union; Human Rights Watch; Electronic Privacy Information Center; Electronic Frontier Foundation; Journalism Education Association; Computer Professionals for Social Responsibility; National Writers Union; Clarinet Communications Corp.; Institute for Global Communications; Stop Prisoner Rape; AIDS Education Global Information System; Bibliobytes; Queer Resources Directory; Critical Path AIDS Project, Inc.; Wildcat Press, Inc.; Declan McCullagh dba Justice on Campus; Brock Meeks dba Cyberwire Dispatch; John Troyer dba The Safer Sex Page; Jonathan Wallace dba The Ethical Spectacle; and Planned Parenthood Federation of America, Inc.

[Footnote 28] American Library Association; America Online, Inc.; American Booksellers Association, Inc.; American Booksellers Foundation for Free Expression; American Society of Newspaper Editors; Apple Computer, Inc.; Association of American Publishers, Inc.; Association of Publishers, Editors and Writers; Citizens Internet Empowerment Coalition; Commercial Internet Exchange Association; CompuServe Incorporated; Families Against Internet Censorship; Freedom to Read Foundation, Inc.; Health Sciences Libraries Consortium; Hotwired Ventures LLC; Interactive Digital Software Association; Interactive Services Association; Magazine Publishers of America; Microsoft Corporation; The Microsoft Network, L. L. C.; National Press Photographers Association; Netcom On Line Communication Services, Inc.; Newspaper Association of America; Opnet, Inc.; Prodigy Services Company; Society of Professional Journalists; Wired Ventures, Ltd.

[Footnote 29] 110 Stat. 142-143, note following 47 U. S. C. A. §223 (Supp.1997).

[Footnote 30] See also 929 F. Supp., at 877: "Four related characteristics of Internet communication have a transcendent importance to our shared holding that the CDA is unconstitutional on its face. We explain these characteristics in our Findings of fact above, and I only rehearse them briefly here. First, the Internet presents very low barriers to entry. Second, these barriers to entry are identical for both speakers and listeners. Third, as a result of these low barriers, astoundingly diverse content is available on the Internet. Fourth, the Internet provides significant access to all who wish to speak in the medium, and even creates a relative parity among speakers." According to Judge Dalzell, these characteristics and therest of the District Court's findings "lead to the conclusion that Congress may not regulate indecency on the Internet at all." Ibid. Because appellees do not press this argument before this Court, we do not consider it. Appellees also do not dispute that the Government generally has a compelling interest in protecting minors from "indecent" and "patently offensive" speech.

[Footnote 31] 390 U.S., at 639. We quoted from Prince v. Massachusetts, 321 U.S. 158, 166 (1944): "It is cardinal with us that the custody, care and nurture of the child reside first in the parents, whose primary function and freedom include preparation for obligations the state can neither supply nor hinder."

[Footnote 32] Given the likelihood that many E mail transmissions from an adult to a minor are conversations between family members, it is therefore incorrect for the dissent to suggest that the provisions of the CDA, even in this narrow area, "are no different from the lawwe sustained in Ginsberg." Post, at 8.

[Footnote 33] Cf. Pacifica Foundation v. FCC, 556 F. 2d 9, 36 (CADC 1977) (Levanthal, J., dissenting), rev'd, FCC v. Pacifica Foundation, 438 U.S. 726 (1978). When Pacifica was decided, given that radio stations were allowed to operate only pursuant to federal license, and that Congress had enacted legislation prohibiting licensees from broadcasting indecent speech, there was a risk that members of the radio audience might infer some sort of official or societal approval of whatever was heard over the radio, see 556 F. 2d, at 37, n. 18. No such risk attends messages received through the Internet, which is not supervised by any federal agency.

[Footnote 34] Juris. Statement 3 (citing 929 F. Supp., at 831 (finding 3)).

[Footnote 35] "Indecent" does not benefit from any textual embellishment at all. "Patently offensive" is qualified only to the extent that it involves "sexual or excretory activities or organs" taken "in context" and "measured by contemporary community standards."

[Footnote 36] See Gozlon Peretz v. United States, 498 U.S. 395, 404 (1991) ("Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion and exclusion") (internal quotation marks omitted).

[Footnote 37] The statute does not indicate whether the "patently offensive" and "indecent" determinations should be made with respect to minors or the population as a whole. The Government asserts that the appropriate standard is "what is suitable material for minors." Reply Brief for Appellants 18, n. 13 (citing Ginsberg v. New York, 390 U.S. 629, 633 (1968)). But the Conferees expressly rejected amendments that would have imposed such a "harmful to minors" standard. See S. Conf. Rep. No. 104-230, p. 189 (1996) (S. Conf. Rep.), 142 Cong. Rec. H1145, H1165-1166 (Feb. 1, 1996). The Conferees also rejected amendments that would have limited the proscribed materials to those lacking redeeming value. See S. Conf. Rep., at 189, 142 Cong. Rec. H1165-1166 (Feb. 1, 1996).

[Footnote 38] Even though the word "trunk," standing alone, might refer to luggage, a swimming suit, the base of a tree, or the long nose of an animal, its meaning is clear when it is one prong of a three part description of a species of gray animals.

[Footnote 39] 413 U.S., at 30 (Determinations of "what appeals to the `prurient interest' or is `patently offensive'. . . . are essentially questions of fact, and our Nation is simply too big and too diverse for this Court to reasonably expect that such standards could be articulated for all 50 States in a single formulation, even assuming the prerequisite consensus exists"). The CDA, which implements the "contemporary community standards" language of Miller, thus conflicts with the Conferees' own assertion that the CDA was intended "to establish a uniform national standard of content regulation." S. Conf. Rep., at 191.

[Footnote 40] Accord, Butler v. Michigan, 352 U.S. 380, 383 (1957) (ban on sale to adults of books deemed harmful to children unconstitutional); Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115, 128 (1989) (ban on "dial a porn" messages unconstitutional); Bolger v. Youngs Drug Products Corp., 463 U.S. 60, 73 (1983) (ban on mailing of unsolicited advertisement for contraceptives unconstitutional).

[Footnote 41] The lack of legislative attention to the statute at issue in Sable suggests another parallel with this case. Compare 492 U.S., at 129-130 ("[A]side from conclusory statements during the debates by proponents of the bill, as well as similar assertions in hearings on a substantially identical bill the year before, . . . the congressional record presented to us contains no evidence as to how effective or ineffective the FCC's most recent regulations were or might prove to be. . . . No Congressman or Senator purported to present a considered judgment with respect to how often or to what extent minors could or would circumvent the rules and have access to dial a porn messages") with n. 24, supra.

[Footnote 42] The Government agrees that these provisions are applicable whenever "a sender transmits a message to more than one recipient, knowing that at least one of the specific persons receiving themessage is a minor." Opposition to Motion to Affirm and Reply to Juris. Statement 4-5, n. 1.

[Footnote 43] The Government asserts that "[t]here is nothing constitutionally suspect about requiring commercial Web site operators . . . to shoulder the modest burdens associated with their use." Brief for Appellants 35. As a matter of fact, however, there is no evidence that a "modest burden" would be effective.

[Footnote 44] Transmitting obscenity and child pornography, whether via the Internet or other means, is already illegal under federal law for both adults and juveniles. See 18 U.S.C. §§ 1464-1465 (criminalizing obscenity); §2251 (criminalizing child pornography). In fact, when Congress was considering the CDA, the Government expressed its view that the law was unnecessary because existing

laws already authorized its ongoing efforts to prosecute obscenity, child pornography, and child solicitation. See 141 Cong. Rec. S8342 (June 14, 1995) (letter from Kent Markus, Acting Assistant Attorney General, U. S. Department of Justice, to Sen. Leahy).

[Footnote 45] Citing Church of Lukumi Babalu Aye, Inc. v. Hialeah, 508 U.S. 520 (1993), among other cases, appellees offer an additional reason why, in their view, the CDA fails strict scrutiny. Because so much sexually explicit content originates overseas, they argue, the CDA cannot be "effective." Brief for Appellees American Library Association et al. 33-34. This argument raises difficult issues regarding the intended, as well as the permissible scope of, extraterritorial application of the CDA. We find it unnecessary to address those issues to dispose of this case.

[Footnote 46] For the full text of §223(e)(5), see n. 26, supra.

[Footnote 47] Thus, ironically, this defense may significantly protect commercial purveyors of obscene postings while providing little (or no) benefit for transmitters of indecent messages that have significant social or artistic value.

[Footnote 48] 929 F. Supp., at 855-856.

[Footnote 49] As this Court long ago explained, "It would certainly be dangerous if the Legislature could set a net large enough to catch all possible offenders and leave it to the courts to step inside and say who could be rightfully be detained and who should be set at large. This would, to some extent, substitute the judicial for the legislative department of the government." United States v. Reese, 92 U.S. 214, 221 (1876). In part because of these separation of powers concerns, we have held that a severability clause is "an aid merely; not an inexorable command." Dorchy v. Kansas, 264 U.S. 286, 290 (1924).

[Footnote 50] See also Osborne v. Ohio, 495 U.S. 103, 121 (1990) (judicial rewriting of statutes would derogate Congress's "incentive to draft a narrowly tailored law in the first place").

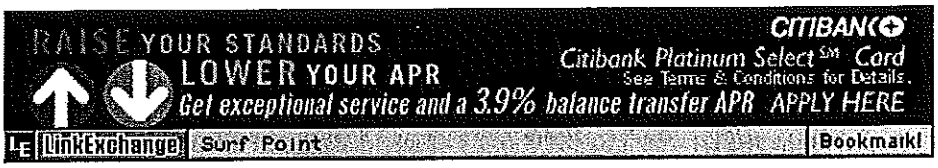
[Footnote 1] See, e.g., Alaska Stat. Ann. §11.66.300 (1996) (no minors in "adult entertainment" places); Ariz. Rev. Stat. Ann. §13-3556 (1989) (no minors in places where people expose themselves); Ark. Code Ann. §§5-27-223, 5-27-224 (1993) (no minors in poolrooms and bars); Colo. Rev. Stat. §18-7-502(2) (1986) (no minors in places displaying movies or shows that are "harmful to children"); Del. Code Ann., Tit. 11, §1365(i)(2) (1995) (same); D. C. Code Ann. §22-2001(b)(1)(B) (1996) (same); Fla. Stat. §847.013(2) (1994) (same); Ga. Code Ann. §16-12-103(b) (1996) (same); Haw. Rev. Stat. §712-1215(1)(b) (1994) (no minors in movie houses or shows that are "pornographic for minors"); Idaho Code §18-1515(2) (1987) (no minors in places displaying movies or shows that are "harmful to minors"); La. Rev. Stat. Ann. §14:91.11(B) (West 1986) (no minors in places displaying movies that depict sex acts and appeal to minors' prurient interest); Md. Ann. Code, Art. 27, §416E (1996) (no minors in establishments where certain enumerated acts are performed or portrayed); Mich. Comp. Laws §750.141 (1991) (no minors without an adult in places where alcohol is sold); Minn. Stat. §617.294 (1987 and Supp. 1997) (no minors in places displaying movies or shows that are "harmful to minors"); Miss. Code Ann. §97-5-11 (1994) (nominors in poolrooms, billiard halls, or where alcohol is sold); Mo. Rev. Stat. §573.507 (1995) (no minors in adult cabarets); Neb. Rev. Stat. §28-809 (1995) (no minors in places displaying movies or shows that are "harmful to minors"); Nev. Rev. Stat. §201.265(3) (1997) (same); N. H. Rev. Stat. Ann. §571-B:2(II) (1986) (same); N. M. Stat. Ann. §30-37-3 (1989) (same); N. Y. Penal Law §235.21(2) (McKinney 1989) (same); N. D. Cent. Code §12.1-27.1-03 (1985 and Supp. 1995) (same); 18 Pa. Cons. Stat. §5903(a) (Supp. 1997) (same); S. D. Comp. Laws Ann. §22-24-30 (1988) (same); Tenn. Code Ann. §39-17-911(b) (1991) (same); Vt. Stat. Ann., Tit. 13, §2802(b) (1974) (same); Va. Code Ann. §18.2-391 (1996) (same).

[Footnote 2] See, e.g., Ala. Code §13A-12-200.5 (1994); Ariz. Rev. Stat. Ann. §13-3506 (1989); Ark. Code Ann. 5-68-502 (1993); Cal. Penal Code Ann. §313.1 (West Supp. 1997); Colo. Rev. Stat. §18-7-502(1) (1986); Conn. Gen. Stat. §53a-196 (1994); Del. Code Ann., Tit. 11, §1365(i)(1) (1995); D. C. Code Ann. §22-2001(b)(1)(A) (1996); Fla. Stat. §847.012 (1994); Ga. Code Ann. §16-12-103(a) (1996); Haw. Rev. Stat. §712-1215(1) (1994); Idaho Code §18-1515(1) (1987); Ill. Comp. Stat., ch. 720, §5/11-21 (1993); Ind. Code §35-49-3-3(1) (Supp. 1996); Iowa Code §728.2 (1993); Kan. Stat. Ann.

§21-4301c(a)(2) (1988); La. Rev. Stat. Ann. §14:91.11(B) (West 1986); Md. Ann. Code, Art. 27, §416B (1996); Mass. Gen. Laws, ch. 272, §28 (1992); Minn. Stat. §617.293 (1987 and Supp. 1997); Miss. Code Ann. §97-5-11 (1994); Mo. Rev. Stat. §573.040 (1995); Mont. Code Ann. §45-8-206 (1995); Neb. Rev. Stat. §28-808 (1995); Nev. Rev. Stat. §§201.265(1), (2) (1997); N. H. Rev. Stat. Ann. §571-B:2(I) (1986); N. M. Stat. Ann. §30-37-2 (1989); N. Y. Penal Law §235.21(1) (McKinney 1989); N. C. Gen. Stat. §14-190.15(a) (1993); N. D. Cent. Code §12.1-27.1-03 (1985 and Supp. 1995); Ohio Rev. Code Ann. §2907.31(A)(1) (Supp. 1997); Okla. Stat., Tit. 21, §1040.76(2) (Supp. 1997); 18 Pa. Cons. Stat. §5903(c) (Supp. 1997); R. I. Gen. Laws §11-31-10(a) (1996); S. C. Code Ann. §16-15-385(A) (Supp. 1996); S. D. Comp. Laws Ann. §22-24-28 (1988); Tenn. Code Ann. §39-17-911(a) (1991); Tex Penal Code Ann. §43.24(b) (1994); Utah Code Ann. §76-10-1206(2) (1995); Vt. Stat. Ann., Tit. 13, §2802(a) (1974); Va. Code Ann. §18.2-391 (1996); Wash. Rev. Code §9.68.060 (1988 and Supp. 1997); Wis. Stat. §948.11(2) (Supp. 1995).

Copyright © 1994-1998 FindLaw Inc.

FindLaw Internet Legal Resources | LegalMinds Community | Laws Cases & Codes | LawReviews Search & Services | LegalNews Today's News | LawCrawler Web Search



FindLaw: Laws: Cases and Codes: 9th Circuit Court Opinions

Search

9th Circuit Court [options]

http://laws.findlaw.com/9th/9755467.html

U.S. 9th Circuit Court of Appeals

PANAVISION INTERNATIONAL v TOEPPEN
9755467

PANAVISION INTERNATIONAL, L.P., a
Delaware Limited Partnership,
No. 97-55467
Plaintiff-Appellee,
D.C. No.
v.
CV-96-03284-DDP-
DENNIS TOEPPEN; NETWORK
JRx
SOLUTIONS, INC., a District of
OPINION
Columbia Corporation,
Defendants-Appellants.

Appeal from the United States District Court
for the Central District of California
Dean D. Pregerson, District Judge, Presiding

Argued and Submitted
March 3, 1998--Pasadena, California

Filed April 17, 1998

Before: Melvin Brunetti, David R. Thompson and
Thomas G. Nelson, Circuit Judges.

Opinion by Judge Thompson

COUNSEL

Joseph D. Murphy, Meyer, Capel, Hirschfeld, Muncy, Jahn &
Aldeen, P.C., Champaign, Illinois, for the defendant-
appellant.

William E. Thomson, Kaye, Scholer, Fierman, Hays & Han-
dler, Los Angeles, California, for the plaintiff-appellee.

OPINION

OPINION

THOMPSON, Circuit Judge:

This case presents two novel issues. We are asked to apply existing rules of personal jurisdiction to conduct that occurred, in part, in "cyberspace." In addition, we are asked to interpret the Federal Trademark Dilution Act as it applies to the Internet.

Panavision accuses Dennis Toeppen of being a "cyber pirate" who steals valuable trademarks and establishes domain names on the Internet using these trademarks to sell the domain names to the rightful trademark owners.

The district court found that under the "effects doctrine," Toeppen was subject to personal jurisdiction in California. Panavision International, L.P. v. Toeppen, 938 F. Supp. 616, 620 (C.D. Cal. 1996). The district court then granted summary judgment in favor of Panavision, concluding that Toeppen's conduct violated the Federal Trademark Dilution Act of 1995, 15 U.S.C. S 1125(c), and the California Anti-dilution statute, California Business & Professions CodeS 14330. Panavision International, L.P. v. Toeppen, 945 F. Supp. 1296, 1306 (C.D. Cal. 1996).

Toeppen appeals. He argues that the district court erred in exercising personal jurisdiction over him because any contact he had with California was insignificant, emanating solely from his registration of domain names on the Internet, which he did in Illinois. Toeppen further argues that the district court erred in granting summary judgment because his use of Panavision's trademarks on the Internet was not a commercial use and did not dilute those marks.

We have jurisdiction under 28 U.S.C. S 1291 and we affirm. The district court's exercise of jurisdiction was proper and comported with the requirements of due process. Toeppen did considerably more than simply register Panavision's trademarks as his domain names on the Internet. He registered those names as part of a scheme to obtain money from Panavision. Pursuant to that scheme, he demanded $13,000 from Panavision to release the domain names to it. His acts were aimed at Panavision in California, and caused it to suffer injury there.

We also conclude Panavision was entitled to summary judgment under the federal and state dilution statutes. Toeppen made commercial use of Panavision's trademarks and his conduct diluted those marks.

I

BACKGROUND

The Internet is a worldwide network of computers that enables various individuals and organizations to share information. The Internet allows computer users to access millions of web sites and web pages. A web page is a computer data file that can include names, words, messages, pictures, sounds, and links to other information.

Every web page has its own web site, which is its address, similar to a telephone number or street address. Every web site on the Internet has an identifier called a "domain name." The domain name often consists of a person's name or a company's name or trademark. For example, Pepsi has a web page with a web site domain name consisting of the company name, Pepsi, and <.com>, the "top level" domain designation:

<Pepsi.com>. 1

The Internet is divided into several "top level " domains: <.edu> for education; <.org> for organizations; <.gov> for government entities; <.net> for networks; and <.com> for "commercial" which functions as the catchall domain for Internet users.

Domain names with the <.com> designation must be registered on the Internet with Network Solutions, Inc. ("NSI"). NSI registers names on a first-come, first-served basis for a $100 registration fee. NSI does not make a determination about a registrant's right to use a domain name. However, NSI does require an applicant to represent and warrant as an express condition of registering a domain name that (1) the applicant's statements are true and the applicant has the right to use the requested domain name; (2) the "use or registration of the domain name . . . does not interfere with or infringe the rights of any third party in any jurisdiction with respect to trademark, service mark, trade name, company name or any other intellectual property right"; and (3) the applicant is not seeking to use the domain name for any unlawful purpose, including unfair competition.

A domain name is the simplest way of locating a web site. If a computer user does not know a domain name, she can use an Internet "search engine." To do this, the user types in a key word search, and the search will locate all of the web sites containing the key word. Such key word searches can yield hundreds of web sites. To make it easier to find their web sites, individuals and companies prefer to have a recognizable domain name.

Panavision holds registered trademarks to the names "Panavision" and "Panaflex" in connection with motion picture camera equipment. Panavision promotes its trademarks through motion picture and television credits and other media advertising.

In December 1995, Panavision attempted to register a web site on the Internet with the domain name <Panavision.com>. It could not do that, however, because Toeppen had already established a web site using Panavision's trademark as his domain name. Toeppen's web page for this site displayed photographs of the City of Pana, Illinois.

On December 20, 1995, Panavision's counsel sent a letter from California to Toeppen in Illinois informing him that Panavision held a trademark in the name Panavision and telling him to stop using that trademark and the domain name <Panavision.com>. Toeppen responded by mail to Panavision in California, stating he had the right to use the name <Panavision.com> on the Internet as his domain name. Toeppen stated:

> If your attorney has advised you otherwise, he is trying to screw you. He wants to blaze new trails in the legal frontier at your expense. Why do you want to fund your attorney's purchase of a new boat (or whatever) when you can facilitate the acquisition of `PanaVision.com' cheaply and simply instead?

Toeppen then offered to "settle the matter" if Panavision would pay him $13,000 in exchange for the domain name. Additionally, Toeppen stated that if Panavision agreed to his offer, he would not "acquire any other Internet addresses which are alleged by Panavision Corporation to be its property."

After Panavision refused Toeppen's demand, he registered Panavision's other trademark with NSI as the domain name <Panaflex.com>. Toeppen's web page for <Panaflex.com> simply displays the word "Hello."

Toeppen has registered domain names for various other companies including Delta Airlines, Neiman Marcus, Eddie Bauer, Lufthansa, and over 100 other marks. Toeppen has attempted to "sell" domain names for other trademarks such as <intermatic.com> to Intermatic, Inc. for $10,000 and <americanstandard.com> to American Standard, Inc. for $15,000.

Panavision filed this action against Toeppen in the District Court for the Central District of California. Panavision alleged claims for dilution of its trademark under the Federal Trademark Dilution Act of 1995, 15 U.S.C. S 1125(c), and under the California Anti-dilution statute, California Business and Professions Code S 14330. Panavision alleged that Toeppen was in the business of stealing trademarks, registering them as domain names on the Internet and then selling the domain names to the rightful trademark owners. The district court determined it had personal jurisdiction over Toeppen, and granted summary judgment in favor of Panavision on both its federal and state dilution claims. This appeal followed.

II

DISCUSSION

A. Personal Jurisdiction

Jurisdiction

A district court's determination that personal jurisdiction can properly be exercised is a question of law reviewable de novo when the underlying facts are undisputed. Fireman's Fund Ins. Co. v. National Bank of Coops., 103 F.3d 888, 893 (9th Cir. 1996). A district court's factual findings regarding jurisdiction are reviewed for clear error. Adler v. Federal Rep. of Nig., 107 F.3d 720, 723 (9th Cir. 1997).

[1] There is no applicable federal statute governing personal jurisdiction in this case. Accordingly, we apply the law of California, the state in which the district court sits. Core-Vent Corp. v. Nobel Industries AB, 11 F.3d 1482, 1484 (9th Cir. 1993). California's long-arm statute permits a court to exercise personal jurisdiction over a defendant to the extent permitted by the Due Process Clause of the Constitution. Cal. Code Civ. P. S 410.10; Gordy v. Daily News, L.P., 95 F.3d 829, 831 (9th Cir. 1996). The issue we address, therefore, is whether the requirements of due process are satisfied by the district court's exercise of personal jurisdiction over Toeppen. Core-Vent, 11 F.3d at 1484.

[2] Personal jurisdiction may be founded on either general jurisdiction or specific jurisdiction.

1. General Jurisdiction

[3] General jurisdiction exists when a defendant is domiciled in the forum state or his activities there are "substantial" or "continuous and systematic." Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 414 -16 (1984). The district court correctly concluded that it did not have general jurisdiction over Toeppen. Toeppen is domiciled in Illinois and his activities in California are not substantial or continuous and systematic. See Toeppen, 938 F. Supp. at 620.

2. Specific Jurisdiction

[4] We apply a three-part test to determine if a district court may exercise specific jurisdiction:

> (1) The nonresident defendant must do some act or consummate some transaction with the forum or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws; (2) the claim must be one which arises out of or results from the defendant's forum-related activities; and (3) exercise of jurisdiction must be reasonable.

Omeluk v. Langsten Slip & Batbyggeri A/S, 52 F.3d 267, 270 (9th Cir. 1995) (quotation omitted).

The first of these requirements is purposeful availment.

a. Purposeful Availment

The purposeful availment requirement ensures that a nonresident defendant will not be haled into court based upon "random, fortuitous or attenuated" contacts with the forum state. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475 (1985). This requirement is satisfied if the defendant "has taken deliberate action" toward the forum state. Ballard v. Savage, 65 F.3d 1495, 1498 (9th Cir. 1995). It is not required that a defendant be physically present or have physical contacts with the forum, so long as his efforts are "purposefully directed" toward forum residents. Id.

i. Application to the Internet

Applying principles of personal jurisdiction to conduct in cyberspace is relatively new. "With this global revolution looming on the horizon, the development of the law concerning the permissible scope of personal jurisdiction based on Internet use is in its infant stages. The cases are scant." Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1123 (W.D. Pa. 1997). We have, however, recently addressed the personal availment aspect of personal jurisdiction in a case involving the Internet. See Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414 (9th Cir. 1997).

In Cybersell, an Arizona corporation, Cybersell, Inc. ("Cybersell AZ"), held a registered servicemark for the name Cybersell. A Florida corporation, Cybersell, Inc. ("Cybersell FL"), created a web site with the domain name <cybsell.com>. The web page had the word "Cybersell" at the top and the phrase, "Welcome to Cybersell!" Id. at 415. Cybersell AZ claimed that Cybersell FL infringed its registered trademark and brought an action in the district court in Arizona. We held the Arizona court could not exercise personal jurisdiction over Cybersell FL, because it had no contacts with Arizona other than maintaining a web page accessible to anyone over the Internet. Id. at 419-420.

In reaching this conclusion in Cybersell, we carefully reviewed cases from other circuits regarding how personal jurisdiction should be exercised in cyberspace. We concluded that no court had ever held that an Internet advertisement alone is sufficient to subject a party to jurisdiction in another state. Id. at 418. In each case where personal jurisdiction was exercised, there had been "something more" to "indicate that the defendant purposefully (albeit electronically) directed his activity in a substantial way to the forum state. " Id. Cybersell

FL had not done this, and the district court could not exercise personal jurisdiction over it.

Personal jurisdiction was properly exercised, however, in CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996). There, the Sixth Circuit held that a Texas resident who had advertised his product via a computer information service, CompuServe, located in Ohio, was subject to personal jurisdiction in Ohio. The court found that the Texas resident had taken direct actions that created a connection with Ohio. Id. at 1264. He subscribed to CompuServe, he loaded his software onto the CompuServe system for others to use, and he advertised his software on the CompuServe system. Id.

[5] In the present case, the district court's decision to exercise personal jurisdiction over Toeppen rested on its determination that the purposeful availment requirement was satisfied by the "effects doctrine." That doctrine was not applicable in our Cybersell case. There, we said: "Likewise unpersuasive is Cybersell AZ's reliance on Panavision International v. Toeppen, 938 F. Supp. 616 (C.D. Cal. 1996), [the district court's published opinion in this case], where the court found the `purposeful availment' prong satisfied by the effects felt in California, the home state of Panavision, from Toeppen's alleged out-of-state scheme to register domain names using the trademarks of California companies, including Panavision, for the purpose of extorting fees from them. Again, there is nothing analogous about Cybersell FL's conduct." Cybersell, 130 F.3d at 420 n.6.

Our reference in Cybersell to "the effects felt in California" was a reference to the effects doctrine.

ii. The Effects Doctrine

[6] In tort cases, jurisdiction may attach if the defendant's conduct is aimed at or has an effect in the forum state. Ziegler v. Indian River County, 64 F.3d 470, 473 (9th Cir. 1995); see Calder v. Jones, 465 U.S. 783 (1984) (establishing an "effects test" for intentional action aimed at the forum state). Under Calder, personal jurisdiction can be based upon: "(1) intentional actions (2) expressly aimed at the forum state (3) causing harm, the brunt of which is suffered--and which the defendant knows is likely to be suffered--in the forum state." Core-Vent Corp. v. Nobel Industries AB, 11 F.3d 1482, 1486 (9th Cir. 1993).

[7] As the district court correctly stated, the present case is akin to a tort case. Panavision, 938 F. Supp. at 621; see also Ziegler, 64 F.3d at 473 (application of the purposeful availment prong differs depending on whether the underlying claim is a tort or contract claim). Toeppen purposefully registered Panavision's trademarks as his domain names on the Internet to force Panavision to pay him money. Panavision, 938 F. Supp. at 621. The brunt of the harm to Panavision was felt in California. Toeppen knew Panavision would likely suffer harm there because, although at all relevant times Panavision was a Delaware limited partnership, its principal place of business was in California, and the heart of the theatrical motion picture and television industry is located there. Id. at 621-622.

The harm to Panavision is similar to the harm to the Indianapolis Colts football team in Indianapolis Colts, Inc. v. Metropolitan Baltimore Football Club Ltd. Partnership, 34 F.3d 410 (7th Cir. 1994). There, the Indianapolis Colts brought a trademark infringement action in the district court in Indiana against the Canadian Football League's new team, the "Baltimore CFL Colts." Id. at 411. The Seventh Circuit held

that the Baltimore CFL Colts team was subject to personal jurisdiction in Indiana even though its only activity directed toward Indiana was the broadcast of its games on nationwide cable television. Id. Because the Indianapolis Colts used their trademarks in Indiana, any infringement of those marks would create an injury which would be felt mainly in Indiana, and this, coupled with the defendant's "entry" into the state by the television broadcasts, was sufficient for the exercise of personal jurisdiction. Id.

Toeppen argues he has not directed any activity toward Panavision in California, much less "entered" the state. He contends that all he did was register Panavision's trademarks on the Internet and post web sites using those marks; if this activity injured Panavision, the injury occurred in cyberspace.2

[8] We agree that simply registering someone else's trademark as a domain name and posting a web site on the Internet is not sufficient to subject a party domiciled in one state to jurisdiction in another. Cybersell, 130 F.3d at 418. As we said in Cybersell, there must be "something more" to demonstrate that the defendant directed his activity toward the forum state. Id. Here, that has been shown. Toeppen engaged in a scheme to register Panavision's trademarks as his domain names for the purpose of extorting money from Panavision. His conduct, as he knew it likely would, had the effect of injuring Panavision in California where Panavision has its principal place of business and where the movie and television industry is centered.3 Under the "effects test," the purposeful availment requirement necessary for specific, personal jurisdiction is satisfied.

b. Defendant's Forum-Related Activities

The second requirement for specific, personal jurisdiction is that the claim asserted in the litigation arises out of the defendant's forum related activities. Ziegler, 64 F.3d at 474. We must determine if the plaintiff Panavision would not have been injured "but for" the defendant Toeppen's conduct directed toward Panavision in California. See Ballard, 65 F.3d at 1500.

[9] This requirement is satisfied. Toeppen's registration of Panavision's trademarks as his own domain names on the Internet had the effect of injuring Panavision in California. But for Toeppen's conduct, this injury would not have occurred. Panavision's claims arise out of Toeppen's California-related activities.

c. Reasonableness

[10] Even if the first two requirements are met, in order to satisfy the Due Process Clause, the exercise of personal jurisdiction must be reasonable. Ziegler, 64 F.3d at 474-75. For jurisdiction to be reasonable, it must comport with "fair play and substantial justice." Burger King, 471 U.S. at 476. "[W]here a defendant who purposefully has directed his activities at forum residents seeks to defeat jurisdiction, he must present a compelling case that the presence of some other considerations would render jurisdiction unreasonable." Core-Vent, 11 F.3d at 1487 (citing Burger King, 471 U.S. at 476-77).

[11] As we have said, Toeppen purposefully directed his activities at Panavision in California. This placed the burden on him to "present a compelling case that the presence of some other considerations would render jurisdiction unreasonable." Id.

[12] In addressing the question of reasonableness, we consider seven factors: (1) the extent of a defendant's purposeful interjection; (2) the burden on the defendant in defending in the forum; (3) the extent of conflict with the sovereignty of the defendant's state; (4) the forum state's interest in adjudicating the dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of the forum to the plaintiff's interest in convenient and effective relief; and (7) the existence of an alternative forum. Burger King, 471 U.S. at 476-77. No one factor is dispositive; a court must balance all seven. Core-Vent, 11 F.3d at 1488.

The district court found that Toeppen had not presented a compelling case that jurisdiction was unreasonable. Panavision, 938 F. Supp. at 622. We agree. The balance of the Burger King factors which we articulated in Core-Vent tips in favor of the exercise of personal jurisdiction.

i. Purposeful Interjection

[13] "Even if there is sufficient`interjection' into the state to satisfy the purposeful availment prong, the degree of interjection is a factor to be weighed in assessing the overall reasonableness of jurisdiction under the reasonableness prong." Core-Vent, 11 F.3d at 1488 (citing Insurance Company of North America v. Marina Salina Cruz, 649 F.2d 1266, 1271 (9th Cir. 1981)). Here, the degree of interjection was substantial.

[14] Toeppen's acts were aimed at Panavision in California. He registered Panavision's trademarks as his domain names, knowing that this would likely injure Panavision in California. In addition, he sent a letter to Panavision in California demanding $13,000 to release his registration of <Panavision.com>. The purposeful interjection factor weighs strongly in favor of the district court's exercise of personal jurisdiction.

ii. Defendant's Burden in Litigating

[15] A defendant's burden in litigating in the forum is a factor in the assessment of reasonableness, but unless the "inconvenience is so great as to constitute a deprivation of due process, it will not overcome clear justifications for the exercise of jurisdiction." Caruth v. International Psychoanalytical Ass'n, 59 F.3d 126, 128-29 (9th Cir. 1995) (citing Roth v. Garcia Marquez, 942 F.2d 617, 623 (9th Cir. 1991)).

[16] The burden on Toeppen as an individual living in Illinois to litigate in California is significant, but the inconvenience is not so great as to deprive him of due process. As the district court stated, " `in this era of fax machines and discount air travel' requiring Toeppen to litigate in California is not constitutionally unreasonable." Panavision, 938 F. Supp. at 622 (quoting Sher v. Johnson, 911 F.2d 1357, 1365 (9th Cir. 1990)).

iii. Sovereignty

[17] This factor concerns the extent to which the district court's exercise of jurisdiction in California would conflict with the sovereignty of Illinois, Toeppen's state of domicile. Core-Vent, 11 F.3d at 1489. Such a conflict is not a concern in this case. The allegations in support of Panavision's state law claim and those in support of its federal claim under the Trademark Dilution Act require the same analysis. The federal analysis would be the same in either Illinois or California. In this circumstance, the exercise of jurisdiction by a federal court in California does not implicate sovereignty concerns of

Illinois.

iv. Forum State's Interest

[18] "California maintains a strong interest in providing an effective means of redress for its residents tortiously injured." Gordy v. Daily News, L.P., 95 F.3d 829, 836 (9th Cir. 1996) (citing Sinatra v. National Enquirer, Inc., 854 F.2d 1191, 1200 (9th Cir. 1988)). Panavision's principal place of business is in California. This factor weighs in Panavision's favor.

v. Efficient Resolution

[19] This factor focuses on the location of the evidence and witnesses. Caruth, 59 F.3d at 129. It is no longer weighed heavily given the modern advances in communication and transportation. Id. In any event, due to the limited amount of evidence and few potential witnesses in the present litigation, this factor is probably neutral.

vi. Convenient & Effective Relief for Plaintiff

[20] In evaluating the convenience and effectiveness of relief for the plaintiff, we have given little weight to the plaintiff's inconvenience. Ziegler, 64 F.3d at 476. It may be somewhat more costly and inconvenient for Panavision to litigate in another forum, but the burden on Panavision is relatively slight. This factor is essentially neutral, perhaps weighing slightly in Toeppen's favor.

vii. Alternative Forum

[21] Panavision has not demonstrated the unavailability of an alternative forum. In this case, Illinois is an alternative forum. As stated above, it may be more costly and inconvenient for Panavision to litigate in Illinois, but this is not an unreasonable burden. This factor weighs in Toeppen's favor.

[22] In balancing the Burger King factors, we conclude that although some factors weigh in Toeppen's favor, he failed to present a compelling case that the district court's exercise of jurisdiction in California would be unreasonable.

[23] We conclude that all of the requirements for the exercise of specific, personal jurisdiction are satisfied. The district court properly exercised personal jurisdiction over Toeppen. We next consider the district court's summary judgment in favor of Panavision on its trademark dilution claims.

B. Trademark Dilution Claims

The Federal Trademark Dilution Act provides:

> The owner of a famous mark shall be entitled . . . to an injunction against another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark . . . .

15 U.S.C. S 1125(c).

The California Anti-dilution statute is similar. See Cal. Bus. & Prof. Code S 14330. It prohibits dilution of "the distinctive quality" of a mark regardless of competition or the likelihood of confusion. The protection extends only to strong and well recognized marks. Panavision's state law dilution claim is subject to the same analysis as its federal claim.

[24] In order to prove a violation of the Federal Trademark Dilution Act, a plaintiff must show that (1) the mark is famous; (2) the defendant is making a commercial use of the mark in commerce; (3) the defendant's use began after the mark became famous; and (4) the defendant's use of the mark dilutes the quality of the mark by diminishing the capacity of the mark to identify and distinguish goods and services. 15 U.S.C. S 1125(c).

Toeppen does not challenge the district court's determination that Panavision's trademark is famous, that his alleged use began after the mark became famous, or that the use was in commerce. Toeppen challenges the district court's determination that he made "commercial use" of the mark and that this use caused "dilution" in the quality of the mark.

1. Commercial Use

[25] Toeppen argues that his use of Panavision's trademarks simply as his domain names cannot constitute a commercial use under the Act. Case law supports this argument. See Panavision International, L.P. v. Toeppen, 945 F. Supp. 1296, 1303 (C.D. Cal. 1996) ("Registration of a trade[mark] as a domain name, without more, is not a commercial use of the trademark and therefore is not within the prohibitions of the Act."); Academy of Motion Picture Arts & Sciences v. Network Solutions, Inc., _____ F. Supp. _____, 1997 WL 810472 (C.D. Cal. Dec. 22, 1997) (the mere registration of a domain name does not constitute a commercial use); Lockheed Martin Corp. v. Network Solutions, Inc., 985 F. Supp. 949 (C.D. Cal. 1997) (NSI's acceptance of a domain name for registration is not a commercial use within the meaning of the Trademark Dilution Act).

Developing this argument, Toeppen contends that a domain name is simply an address used to locate a web page. He asserts that entering a domain name on a computer allows a user to access a web page, but a domain name is not associated with information on a web page. If a user were to type <Panavision.com> as a domain name, the computer screen would display Toeppen's web page with aerial views of Pana, Illinois. The screen would not provide any information about "Panavision," other than a "location window " which displays the domain name. Toeppen argues that a user who types in <Panavision.com>, but who sees no reference to the plaintiff Panavision on Toeppen's web page, is not likely to conclude the web page is related in any way to the plaintiff, Panavision.

[26] Toeppen's argument misstates his use of the Panavision mark. His use is not as benign as he suggests. Toeppen's "business" is to register trademarks as domain names and then sell them to the rightful trademark owners. He "act[s] as a `spoiler,' preventing Panavision and others from doing business on the Internet under their trademarked names unless they pay his fee." Panavision, 938 F. Supp. at 621. This is a commercial use. See Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1230 (N.D. Ill. 1996) (stating that "[o]ne of Toeppen's business objectives is to profit by the resale or licensing of these domain names, presumably to the entities who conduct business under these names.").

[27] As the district court found, Toeppen traded on the value of Panavision's marks. So long as he held the Internet registrations, he curtailed Panavision's exploitation of the value of its trademarks on the Internet, a value which Toeppen then used when he attempted to sell the <Panavision.com> domain name to Panavision.

In a nearly identical case involving Toeppen and Intermatic

Inc., a federal district court in Illinois held that Toeppen's conduct violated the Federal Trademark Dilution Act. Intermatic, 947 F. Supp. at 1241. There, Intermatic sued Toeppen for registering its trademark on the Internet as Toeppen's domain name, <intermatic.com>. It was "conceded that one of Toeppen's intended uses for registering the Intermatic mark was to eventually sell it back to Intermatic or to some other party." Id. at 1239. The court found that "Toeppen's intention to arbitrage the `intermatic.com' domain name constitute[d] a commercial use." Id. See also Teletech Customer Care Management, Inc. v. Tele-Tech Co., 977 F. Supp. 1407 (C.D. Cal. 1997) (granting a preliminary injunction under the Trademark Dilution Act for use of a trademark as a domain name).

Toeppen's reliance on Holiday Inns, Inc. v. 800 Reservation, Inc., 86 F.3d 619 (6th Cir. 1996), cert. denied, 117 S. Ct. 770 (1997) is misplaced. In Holiday Inns, the Sixth Circuit held that a company's use of the most commonly misdialed number for Holiday Inns' 1-800 reservation number was not trademark infringement.

Holiday Inns is distinguishable. There, the defendant did not use Holiday Inns' trademark. Rather, the defendant selected the most commonly misdialed telephone number for Holiday Inns and attempted to capitalize on consumer confusion.

A telephone number, moreover, is distinguishable from a domain name because a domain name is associated with a word or phrase. A domain name is similar to a "vanity number" that identifies its source. Using Holiday Inns as an example, when a customer dials the vanity number "1-800-Holiday," she expects to contact Holiday Inns because the number is associated with that company's trademark. A user would have the same expectation typing the domain name <HolidayInns.com>. The user would expect to retrieve Holiday Inns' web page.4

[28] Toeppen made a commercial use of Panavision's trademarks. It does not matter that he did not attach the marks to a product. Toeppen's commercial use was his attempt to corporation." Id. at 95.

sell the trademarks themselves.5 Under the Federal Trademark Dilution Act and the California Anti-dilution statute, this was sufficient commercial use.

2. Dilution

[29] "Dilution" is defined as "the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of (1) competition between the owner of the famous mark and other parties, or (2) likelihood of confusion, mistake or deception. " 15 U.S.C. S 1127.6

Trademark dilution on the Internet was a matter of Congressional concern. Senator Patrick Leahy (D-Vt.) stated:

> [I]t is my hope that this anti-dilution statute can help stem the use of deceptive Internet addresses taken by those who are choosing marks that are associated with the products and reputations of others.

141 Cong. Rec. S 19312-01 (daily ed. Dec. 29, 1995) (statement of Sen. Leahy). ~~See also Teletech Customer Care Man-~~ with ~~this case stems from the fact that a reproduction of the trademark~~ itself is being sold, unattached to any other goods or services." ~~Id. at 1010.~~

The court concluded that trademark law should protect the trademark itself. "Although our decision here may slightly tilt the trademark laws from the purpose of protecting the public to the protection of the business interests of plaintiffs, we think that the two become . . . intermeshed . . . ." Id. at 1011. "Whereas traditional trademark law sought primarily to protect consumers, dilution laws place more emphasis on protecting the investment of the trademark owners." Panavision, 945 F. Supp. at 1301.
6 The Lanham Act, 15 U.S.C. S 1127, provides definitions for the Trademark Dilution Act, 15 U.S.C. S 1125(c).

agement, Inc. v. Tele-Tech Co., Inc., 977 F. Supp. 1407, 1413 (C.D. Cal. 1997).

To find dilution, a court need not rely on the traditional definitions such as "blurring" and "tarnishment."7 Indeed, in concluding that Toeppen's use of Panavision's trademarks diluted the marks, the district court noted that Toeppen's conduct varied from the two standard dilution theories of blurring and tarnishment. Panavision, 945 F. Supp. at 1304. The court found that Toeppen's conduct diminished "the capacity of the Panavision marks to identify and distinguish Panavision's goods and services on the Internet." Id. See also Intermatic, 947 F. Supp. at 1240 (Toeppen's registration of the domain name, "lessens the capacity of Intermatic to identify and distinguish its goods and services by means of the Internet.").

This view is also supported by Teletech. There, TeleTech Customer Care Management Inc., ("TCCM"), sought a preliminary injunction against Tele-Tech Company for use of TCCM's registered service mark, "TeleTech," as an Internet domain name. Teletech, 977 F. Supp. at 1410. The district court issued an injunction, finding that TCCM had demonstrated a likelihood of success on the merits on its trademark dilution claim. Id. at 1412. The court found that TCCM had invested great resources in promoting its servicemark and Teletech's registration of the domain name <teletech.com> on the Internet would most likely dilute TCCM's mark. Id. at 1413.

Toeppen argues he is not diluting the capacity of the Panavision marks to identify goods or services. He contends that even though Panavision cannot use <Panavision.com> and <Panaflex.com> as its domain name addresses, it can still promote its goods and services on the Internet simply by using some other "address" and then creating its own web page using its trademarks.

[30] We reject Toeppen's premise that a domain name is nothing more than an address. A significant purpose of a domain name is to identify the entity that owns the web site.8 "A customer who is unsure about a company's domain name will often guess that the domain name is also the company's name." Cardservice Int'l v. McGee, 950 F. Supp. 737, 741 (E.D. Va. 1997). "[A] domain name mirroring a corporate name may be a valuable corporate asset, as it facilitates communication with a customer base." MTV Networks, Inc. v. Curry, 867 F. Supp. 202, 203-204 n.2 (S.D.N.Y. 1994).

[31] Using a company's name or trademark as a domain name is also the easiest way to locate that company's web site. Use of a "search engine" can turn up hundreds of web sites, and there is nothing equivalent to a phone book or directory assistance for the Internet. See Cardservice, 950 F. Supp. at 741.

[32] Moreover, potential customers of Panavision will be discouraged if they cannot find its web page by typing in "<Panavision.com," but instead are forced to wade through hundreds of web sites. This dilutes the value of Panavision's

trademark. We echo the words of Judge Lechner, quoting Judge Wood: "Prospective users of plaintiff's services who mistakenly access defendant's web site may fail to continue to search for plaintiff's own home page, due to anger, frustration or the belief that plaintiff's home page does not exist." Jews for Jesus v. Brodsky, _____F. Supp. _____, No. CIV A. 98-274 (AJL), 1998 WL 111676 (D.N.J., Mar. 6, 1998) at *22 (Lechner, J., quoting Wood, J. in Planned Parenthood, 1997 WL 133313 at *4); see also Teletech, 977 F. Supp. at 1410 (finding that use of a search engine can generate as many as 800 to 1000 matches and it is "likely to deter web browsers from searching for Plaintiff's particular web site").

[33] Toeppen's use of <Panavision.com> also puts Panavision's name and reputation at his mercy. See Intermatic, 947 F. Supp. at 1240 ("If Toeppen were allowed to use`intermatic.com,' Intermatic's name and reputation would be at Toeppen's mercy and could be associated with an unimaginable amount of messages on Toeppen's web page.").

[34] We conclude that Toeppen's registration of Panavision's trademarks as his domain names on the Internet diluted those marks within the meaning of the Federal Trademark Dilution Act, 15 U.S.C. S 1125(c), and the California Anti-dilution statute, Cal.Bus. & Prof. Code S 14330.

III

CONCLUSION

Toeppen engaged in a scheme to register Panavision's trademarks as his domain names on the Internet and then to extort money from Panavision by trading on the value of those names. Toeppen's actions were aimed at Panavision in California and the brunt of the harm was felt in California. The district court properly exercised personal jurisdiction over Toeppen.

We also affirm the district court's summary judgment in favor of Panavision under the Federal Trademark Dilution Act, 15 U.S.C. S 1125(c), and the California Anti-dilution statute, Cal.Bus. & Prof. Code S 14330. Toeppen made commercial use of Panavision's trademarks and his conduct diluted those marks.

AFFIRMED. the end

FOOTNOTES

1 We use the arrow keys (< >) to set out a domain name or a web site. These arrows are not part of the name or the site.
2 In a subset of this argument, Toeppen contends that a large organization such as Panavision does not suffer injury in one location. See Cybersell, 130 F.3d at 420 (A corporation "does not suffer harm in a particular geographic location in the same sense that an individual does.") However, in Core-Vent, we stated that Calder v. Jones, 465 U.S. 783 (1984), does not preclude a determination that a corporation suffers the brunt of harm in its principal place of business. Core-Vent, 11 F.3d at 1487. Panavision was previously a limited partnership and is now a corporation. Under either form of business organization, however, the brunt of the harm suffered by Panavision was in the state where it maintained its principal place of business, California.
3 We discuss the nature of Panavision's injury in following Part B.
4 See Carl Oppedahl, Analysis and Suggestions Regarding NSI Domain Name Trademark Dispute Policy, 7 Fordham Intell. Prop. Media & Ent.

5 See Boston Pro. Hockey Assoc., Inc. v. Dallas Cap & Emblem Mfg.,

Inc., 510 F.2d 1004 (1975), which involved the sale of National Hockey

7 Blurring occurs when a defendant uses a plaintiff's trademark to identify the defendant's goods or services, creating the possibility that the mark will lose its ability to serve as a unique identifier of the plaintiff's product. Ringling Bros.-Barnum & Bailey, Combined Shows, Inc. v. B.E. Windows, Corp., 937 F. Supp. 204, 209 (S.D.N.Y. 1996) (citing Deere & Co. v. MTD Prods., Inc., 41 F.3d 39, 43 (2d. Cir. 1994)); Thomas McCarthy, McCarthy on Trademarks and Unfair Competition, S 24:68 at 24-111 (4th ed. 1997); see also Ringling Bros.-Barnum & Bailey Combined Shows, Inc. v. Utah Div. of Travel Development, 955 F. Supp. 605, 614-15 (E.D. Va. 1997) (discussing the inadequacies of current definitions of blurring and determining that blurring requires consumers to mistakenly associate a defendant's mark with a plaintiff's famous trademark).

Tarnishment occurs when a famous mark is improperly associated with an inferior or offensive product or service. McCarthy, S 24:104 at 24-172 to 173; Ringling Bros., 937 F. Supp. at 209 (citing Hormel Foods Corp. v. Jim Henson Prods., Inc., 73 F.3d 497, 506 (2d. Cir. 1996)).

8 This point was made in a recent legal periodical:

> The domain name serves a dual purpose. It marks the location of the site within cyberspace, much like a postal address in the real world, but it may also indicate to users some information as to the content of the site, and, in instances of well-known trade names or trademarks, may provide information as to the origin of the contents of the site.

Peter Brown, New Issues in Internet Litigation, 17th Annual Institute on Computer Law: The Evolving Law of the Internet-Commerce, Free Speech, Security, Obscenity and Entertainment, 471 Prac. L. Inst. 151 (1997).

2ND CASE of Level 2 printed in FULL format.

PLAYBOY ENTERPRISES, INC., a Delaware corporation, Plaintiff, v. TERRI WELLES, Defendant.

CASE NO. 98-CV-0413-K (JFS)

UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF CALIFORNIA

7 F. Supp. 2d 1098; 1998 U.S. Dist. LEXIS 9180; 47 U.S.P.Q.2D (BNA) 1186; 98 Daily Journal DAR 8613

May 20, 1998, Decided
May 21, 1998, Filed

DISPOSITION: [**1] Plaintiff's Motion for a Preliminary Injunction DENIED.

CORE TERMS: trademark, playboy, website, magazine, dilution, preliminary injunction, fair use, infringement, websurfer, tags, meta, causes of action, customer, site, web, Lanham Act, abbreviation, consumer, famous, disclaimer, good faith, trademark infringement, unfair competition, designation, descriptive, distinctive, endorsed, logo, font, trademarked

COUNSEL: Craig Courter, Seltzer, Caplan, Wilkins & McMahon, San Diego, CA, for plaintiff.

David R. Francescani, Amy Benjamin, and Maryann V. Hayes, Darby & Darby, New York, NY, for plaintiff.

hael J. Plonsker, Max J. Sprecher, and Anne Kearns, Lavely & Singer, Los Angeles, CA, for defendant.

JUDGES: Judge Judith N. Keep, United States District Court, Southern District of California.

OPINIONBY: Judith N. Keep

OPINION: [*1099] AMENDED ORDER DENYING PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION

On February 27, 1998, plaintiff Playboy Enterprises, Inc. (PEI) filed a Complaint against defendant Terri Welles. The Complaint consists of five causes of action: 1) trademark infringement pursuant to 15 U.S.C. @ 1114(1); n1 2) false designation of [*1100] origin and unfair competition under 15 U.S.C. @ 1125(a); n2 3) dilution of trademarks pursuant to 15 U.S.C. 1125(c); 4) trademark infringement and unfair competition under California common law; 5) unfair competition in violation of Cal. Bus. & Prof. Code @ 17200, et seq.

- - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n1 Title 15 U.S.C. @ 1114(1)(a) reads as follows: "Any person who shall, without the consent of the registrant use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion,

or to cause mistake, or to deceive . . . shall be liable in a civil action by the registrant for the remedies hereinafter provided." [**2]

n2 Title 15 U.S.C. @ 1125(a)(1)(A) reads as follows: "Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person. . . shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act."

- - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - -

On March 18, 1998, plaintiff filed a Motion for Preliminary Injunction. Defendant filed an Opposition on April 6, 1998. Plaintiff filed its Reply on April 13, 1998. The court heard oral arguments on April 20, 1998.

I. BACKGROUND

The following background facts are taken from the parties' contentions in their papers, but the court does [**3] not make any ultimate findings of fact with respect to this case. Plaintiff Playboy Enterprises, Inc. (PEI) is an international publishing and entertainment company. Since 1953, PEI has published Playboy magazine, a widely popular magazine with approximately ten (10) million readers each month. PEI also publishes numerous specialty magazines such as Playboy's Playmate Review, Playboy's Playmates of the Year, and Playboy's Calendar Playmates among other publications. In addition to its publishing ventures, PEI produces television programming for cable and direct-to-home satellite transmission and sells and licenses various goods and services including videos.

PEI has established two websites. According to plaintiff, its free website, http://www.playboy.com, has become one of the most popular sites on the Web and is used to promote its magazine, goods, and services. Its other website, called the "Playboy Cyber Club," http://www.cyber.playboy.com, is devoted to promoting current and former PEI models.

PEI owns federally registered trademarks for the terms Playboy, Playmate, Playmate of the Month, and Playmate of the Year. The term Playmate of the Year is sometimes [**4] abbreviated "PMOY." PEI does not have a federally registered trademark in the abbreviation "PMOY," although PEI argues that "PMOY" is worthy of trademark protection because it is a well-known abbreviation for the trademark Playmate of the Year.

Defendant Terri Welles is a self-employed model and spokesperson, who began her modeling career with Playboy magazine in 1980. In May of 1980, Ms. Welles appeared on the cover of Playboy magazine and was subsequently featured as the "Playmate of the Month" in the December 1980 issue. Ms. Welles received the "Playmate of the Year" award in June of 1981. Since 1980, Ms. Welles has appeared in no less than thirteen (13) issues of Playboy magazine and eighteen (18) newsstand specials published by PEI. Defendant claims that she has always

referred to herself since 1980 as a "Playmate" or "Playmate of the Year" with knowledge of PEI.

On June 29, 1997, Ms. Welles opened a website, http://www.terriwelles.com, which includes photographs of herself and others (both nude and clothed), a fan club posting board, an autobiography section, and a listing of current events and personal appearances. The domain name for defendant's site is [**5] "terriwelles," the heading for the website is "Terri Welles--Playmate of the Year 1981," and title of the link page is "Terri Welles--Playboy Playmate of the Year 1981." Each of the pages uses "PMOY '81" as a repeating watermark in the background. According to defendant, eleven (11) of the fifteen (15) free web pages include a disclaimer at the bottom of the pages, in varying font sizes depending on the page, which indicates that the website is not endorsed by PEI; the disclaimer reads as follows: "This site is neither endorsed, nor sponsored by, nor affiliated with Playboy Enterprises, [*1101] Inc. PLAYBOY, PLAYMATE OF THE YEAR and PLAYMATE OF THE MONTH are registered trademarks of Playboy Enterprises, Inc." Defendant uses the terms Playboy and Playmate along with other terms within the keywords section of the meta tags, which constitutes the internal index of the website used by some search engines.

The site contains link pages to other erotic, adult-oriented websites. It also contains advertising "banners" for some of those websites.

Since May of 1997, defendant has been in contact with plaintiff about the design and creation of her website. Defendant claims that plaintiff, through [**6] Marcia Terrones, the director of the "Rights and Permission" department at PEI, informed her that she could identify herself as the "Playmate of the Year 1981" but that she could not reproduce the rabbit head logo on her proposed site. Various communications between defendant and plaintiff ensued. According to defendant, PEI, through Hug Hefner, initially complimented her website and encouraged her use of the title "Playmate of the Year 1981." However, Mr. Hefner later informed defendant that use of PEI's trademarks were restricted; instead, he invited defendant to join PEI's new Cyber Club. Defendant refused this invitation, and PEI continued to demand that defendant remove the "Playmate of the Year" title from the home page as well as remove the PMOY watermark from the background.

Plaintiff has moved for a preliminary injunction which would enjoin defendant from 1) using the trademarked term Playmate of the Year in the title of the home page and the link page; 2) from using the watermark "PMOY '81" in the background; and 3) from using the trademarked terms Playboy and Playmate in the meta-tagging of defendant's site. Therefore, the task before the court is to determine [**7] whether a preliminary injunction against defendant is warranted in this instance.

II. STANDARD OF LAW

To be entitled to a preliminary injunction, a party must show either (1) a combination of probable success on the merits and a possibility of irreparable harm, or (2) the existence of serious questions on the merits and the balance of hardships weighing heavily in its favor. Vision Sports v. Melville, 888 F.2d 609, 612 (9th Cir. 1988). These are not two distinct tests, but ends of a continuum in which the required showing of harm "varies inversely with the required showing of meritoriousness." Rodeo Collection v. West Seventh, 812

F.2d 1215, 1217 (9th Cir. 1987) (citation omitted). "Thus, a moving party need not demonstrate that [it] risks irreparable injury, but [it] must at least show that [it] will suffer a degree of hardship that outweighs the hardship facing the opposing party if the injunction is not issued. Similarly, a moving party need not demonstrate that [it] will succeed on the merits, but must at least show that [its] cause presents serious questions of law worthy of litigation." Topanga Press, Inc. v. City of L.A., 989 F.2d 1524, [**8] 1528 (9th Cir. 1993).

III. DISCUSSION

In general, plaintiff argues that defendant's use of the Playboy and Playmate trademarks in conjunction with her website is likely to cause confusion, mistake or deception. See Complaint at P 32. Specifically, PEI avers that these alleged infringements are harming it and its trademarks since websurfing consumers are likely to believe that defendant's website is authorized, sponsored or otherwise approved by PEI when it is not. Id. Defendant, on the other hand, contends that her use of the title Playmate of the Year and the abbreviation PMOY is merely a descriptive use of those terms so as to identify herself to her customers. She argues that any other use of PEI's trademarked terms is merely used in an editorial fashion.

In this motion, plaintiff concentrates on defendant's use of the Playmate of the Year title in Ms. Welles' web page heading and link page, her use of the PMOY '81 term as a watermark in the web page background, and her use of the Playboy and Playmate marks as meta tags. These appear to be the only infringements alleged by PEI; accordingly, the court will focus on these three [**9] particular issues in this order.

Based on these alleged infringements, plaintiff states five causes of action against [*1102] defendant in its Complaint. However, in this motion, PEI moves for a preliminary injunction on the basis of only three of those causes of action: (First Cause of Action) federal trademark infringement; (Second Cause of Action) false designation of origin under section 43(a) of the Lanham Act; and (Third Cause of Action) dilution under section 43(c) of the Lanham Act. Defendant refers to the first two causes of action as the trademark causes of action and can be treated together. Plaintiff does not make direct reference to the remaining causes of action which are related state law causes of action. Therefore, the court will not address those issues. The court will now address whether a preliminary injunction is warranted in this case.

A. Irreparable Harm

"In copyright and trademark cases, irreparable injury is presumed upon a showing of likelihood of success." Dr. Seuss Enters. v. Penguin Book USA, Inc., 924 F. Supp. 1559, 1574 (S.D. Cal. 1996), aff'd, 109 F.3d 1394 (9th Cir. 1997). Thus, the court will examine the plaintiff's likelihood of success [**10] on the three causes of action upon which it relies.

B. Likelihood of Success in Trademark Causes of Action

Plaintiff asserts that defendant is infringing on its registered trademarks in violation of Section 32(1) of the Lanham Act, 15 U.S.C. @ 1114(1), and that said infringement is causing confusion, mistake, or deception which

constitutes false designation of origin and unfair competition in violation of section 43(a) of the Lanham Act, 15 U.S.C. @ 1125(a). The purpose of a trademark is to allow for customer identification of the manufacturer or sponsor of a good or the provider of a service. See New Kids on the Block v. New Am. Pub., Inc., 971 F.2d 302, 305 (9th Cir. 1992).

It is undisputed that PEI owns federally-registered trademarks for the words Playboy, Playmate, Playmate of the Month, and Playmate of the Year. The term Playboy has gained widespread public recognition and is distinctive due in large part to the long-standing success and popularity of Playboy magazine and related publications from PEI. See Playboy Enters., Inc. v. Chuckleberry Publishing, Inc., 687 F.2d 563, 566-67 (2d Cir. 1982) (holding that the Playboy mark is distinctive, [**11] widely recognized, and of great value). However, the other trademarks such as Playmate are not only trademarks related to Playboy magazine, but they are titles bestowed upon particular models who appear in that magazine. From the papers submitted and the oral arguments, it appears that the terms Playmate, Playmate of the Month, and Playmate of the Year are titles which Playboy magazine awards to certain Playboy models, who then use the title to describe themselves. Much like Academy Award winners, crowned Miss Americas, and Heisman Trophy winners, Playboy Playmates are given a title which becomes part of their identity and adds value to their name. Indisputably, these winners represent the awarding organization or sponsor, but the title becomes part of who they are to the public.

In the case of Playboy Playmates, PEI encourages these select models to use their titles for their self-promotion and the promotion of its magazines and assorted goods and services. In the case of Ms. Welles, it appears that PEI had no objection to her use of the terms Playmate of the Year or Playboy Playmate until she launched her competing website. n3 In oral argument, [**12] PEI conceded that these models may use their title for their own benefit, as in the title of an autobiography. PEI also admitted that Ms. Welles is not contractually restricted from using the terms Playmate of the Month or Playmate of the Year based on her previous [*1103] contracts with PEI. However, it contends that Ms. Welles may not trade on PEI's marks so as to compete with PEI; specifically, PEI argues that the prominent use of its marks to attract the attention of potential customers is a trademark infringement as well as a dilution of its marks.

- - - - - - - - - - - - - - - - - - -Footnotes- - - - - - - - - - - - - - - - - -

n3 Defendant raises the issue of PEI's acquiescence in Ms. Welles' use of the terms Playmate, Playmate of the Month, and Playmate of the Year. Plaintiff does not contest that it allowed defendant to use these terms previously, but it argues that the defense of acquiescence does not apply in this case since defendant is now engaged in a competitive "trademark use" of those terms. "The defense of acquiescence is a type of estoppel which constitutes a ground for denial of relief upon a finding of conduct on plaintiff's part that amounts to an assurance by the plaintiff to the defendant, either express or implied that plaintiff will not assert his trademark rights against the defendant." CBS Inc. v. Man's Day Publishing Company, Inc., 205 U.S.P.Q. 470, 473-74 (1980). The court does not find it necessary to decide if this defense is applicable in this case.

- - - - - - - - - - - - - - - - - - -End Footnotes- - - - - - - - - - - - - - - - - -

- [**13]

In the papers submitted, the parties engage in an extensive analysis of whether defendant's use of PEI's trademarks creates confusion among websurfers. Indeed, the dispositive legal issue in the standard trademark case concerns "customer confusion." See WCVB-TV v. Boston Athletic Ass'n, 926 F.2d 42, 44 (1st Cir. 1991). The Ninth Circuit has articulated an eight-factor test which the court may consider in determining the likelihood of confusion: 1) the strength of the mark; 2) proximity or relatedness of the goods; 3) similarity in appearance, sound, and meaning of the marks; 4) evidence of actual confusion; 5) degree to which the marketing channels converge; 6) type of good and degree of care customers are likely to exercise in purchasing them; 7) evidence of the intention of defendant in selecting and using the alleged infringing name; and 8) likelihood that the parties will expand their product lines. See Metro Pub. Ltd. v. San Jose Mercury News, 987 F.2d 637, 640 (9th Cir. 1993); see also Century 21 Real Estate Corp. v. Sandlin, 846 F.2d 1175, 1178-79 (9th Cir. 1988) (applying a similar six-factor test). These factors are simply helpful guidelines for the determination [**14] of potential customer confusion. See Metro Pub., 987 F.2d at 640.

This case, however, is not a standard trademark case and does not lend itself to the systematic application of the eight factors. In the case at bar, defendant has used the terms Playmate of the Year and its abbreviation PMOY on her website. She has also used the terms Playboy and Playmate as meta tags for her site so that those using search engines on the Web can find her website if they were looking for a Playboy Playmate. The problem in this case is that the trademarks that defendant uses, and the manner in which she uses them, describe her and identify her. This raises a question of whether there is a "fair use" of these marks pursuant to 15 U.S.C. @@ 1115(b)(4) and 1125(c)(4). See New Kids, 971 F.2d at 306 (noting that the "fair use" defense arises when the trademark also describes a person, a place or an attribute of a product). Terri Welles was and is the "Playmate of the Year for 1981." Plaintiff has conceded this fact and has not submitted any evidence for the court to conclude that PEI may prevent defendant from using that term to identify herself and her award; as noted above, [**15] PEI conceded that there are no contractual agreements between it and defendant which restrict her use of any of the marks. Thus, defendant has raised a "fair use" defense which must be overcome by the plaintiff before a potential infringement under Section 43(a) of the Lanham Act or trademark dilution under Section 43(c) of the Lanham Act may be found.

In a case where the "mark is used only to 'describe the goods or services of [a] party, or their geographic origin,' trademark law recognizes a "fair use" defense. Id. (quoting 15 U.S.C. @ 1115(b)(4)). Title 15 U.S.C. @ 1115(b)(4) states the following:

That the use of the name, term, or device charged to be an infringement is a use, otherwise than as a mark, of the party's individual name in his own business, or of the individual name of anyone in privity with such party, or of a term or device which is descriptive of and used fairly and in good faith only to describe the goods or services of such party, or their geographic origin. . . .

Id. "'The 'fair use' defense, in essence, forbids a trademark registrant to appropriate a descriptive term for his exclusive use and so prevent others

from accurately describing [**16] a characteristic of their goods.'" New [illegible], 971 F.2d at 306 (quoting Soweco, Inc. v. Shell Oil Co., 617 F.2d 1178, 1185 (5th Cir. 1980)). In the case at bar, Ms. Welles has used the trademark term Playmate of the Year to identity and describe herself. As the court noted above, Ms. Welles earned the title of "Playboy Playmate of the Year" in 1981 and has used that title ever since, without objection from PEI.

From the exhibits submitted with the parties' papers and presented at oral argument, it is evident that Ms. Welles has minimized her references to Playboy on her website and has not attempted to trick consumers [*1104] into believing that they are viewing a Playboy-endorsed website. In Volkswagenwerk Aktiengesellschaft v. Church, 411 F.2d 350, 352 (9th Cir. 1969), the Ninth Circuit held that the defendant was able to advertise that he repaired Volkswagen vehicles as long as he did not do so in a manner "which is likely to suggest to his prospective customers that he is part of Volkswagen's organization of franchised dealers and repairmen." Id. In the case at bar, Ms. Welles has noted created a Playboy-related website. She does not use Playboy or Playmate [**17] in her domain name, she does not use the classic Playboy bunny logo, she inserted disclaimers which clearly state that the website is not endorsed by PEI, and the font of the Playmate of the Year 1981 title is not recognizable as a Playboy magazine font.

It is clear that defendant is selling Terri Welles and only Terri Welles on the website. There is no overt attempt to confuse the websurfer into believing that her site is a Playboy-related website. In this case, then, defendant's use of the term Playmate of the Year 1981 "is descriptive of and used fairly and in good faith only to describe [herself]." 15 U.S.C. @ 1115(b)(4). As such, the use of the abbreviation PMOY '81 is also permissible since it makes reference to her title as "Playmate of the Year 1981." Since the court finds that "PMOY '81" is a fair description of Ms. Terri Welles, it is not necessary to rule on whether the abbreviation PMOY is a protected trademark.

With respect to the meta tags, the court finds there to be no trademark infringement where defendant has used plaintiff's trademarks in good faith to index the content of her website. The meta tags are not visible to the websurfer although [**18] some search engines rely on these tags to help websurfers find certain websites. Much like the subject index of a card catalog, the meta tags give the websurfer using a search engine a clearer indication of the content of a website. The use of the term Playboy is not an infringement because it references not only her identity as a "Playboy Playmate of the Year 1981," but it may also reference the legitimate editorial uses of the term Playboy contained in the text of defendant's website. Plaintiff conceded, both in its papers and in oral argument, that defendant may properly use the term Playboy in an editorial fashion (i.e. in reference to the Playboy Mansion). Therefore, the court finds that defendant has not infringed on defendant's trademarks by using them in her website meta tags.

Since defendant is entitled to the "fair use" defense pursuant to 15 U.S.C. @ 1115(b)(4), it is not necessary to determine the likelihood of confusion in this case. However, even if the court were to determine the likelihood of confusion in this case, it does not appear that there is a likelihood that websurfers would think that Ms. Welles' website is endorsed or sanctioned in any way [**19] by PEI. Even if Ms. Welles were not entitled to the fair use defense, plaintiff has failed to demonstrate that there is a likelihood of confusion

for websurfers. Certainly, the PEI trademarks are strong and are used by PEI to sell adult entertainment on the Internet. Defendant claims she is selling a different class of goods since she is offering her promotional services and related goods like her line of cigars. However, it appears that PEI and Terri Welles are in competition for websurfers who pay money for on-line erotica, regardless of the underlying promotion.

Other factors weigh in defendant's favor. Though she is using the trademarks, she has done nothing else to make her use identical to the Playboy trademark. There is no bunny logo, the font for the terms is different, and there is no other indication that PEI is sponsoring the website. Plaintiff has presented no empirical evidence to show that there is actual confusion among consumers. Though not necessary, the lack of any such demonstration weighs in defendant's favor. Finally, it appears that defendant has used the trademarks in good faith. She has removed some of the references per PEI's request, has not used the [**20] bunny logo, and has added a disclaimer to the vast majority of her free web pages. See Consumers Union of U.S. v. General Signal Corp., 724 F.2d 1044, 1053 (2d Cir. 1983) ("Disclaimers are a favored way of alleviating consumer confusion as to source or sponsorship."). This indicates good faith in the use of the trademarks and weighs in favor of defendant. Hence, even if the court were to apply the Ninth Circuit's eight-factor test, plaintiff has [*1105] failed to demonstrate that it would likely succeed in proving that defendant's use of the trademarks causes a likelihood of confusion for the consumer. As the court has already noted, the Terri Welles web page appears to promote Terri Welles only and makes no attempt to connect itself with Playboy or PEI.

C. Dilution Claim

Given that the court has found that defendant is entitled to the "fair use" defense pursuant to 15 U.S.C. @ 1115(b)(4), plaintiff cannot make a sufficient dilution claim under 15 U.S.C. @ 1125(c) to warrant the granting of a preliminary injunction. Dilution is defined as "the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence [**21] of . . . (2) likelihood of confusion, mistake, or deception." 15 U.S.C. @ 1127. Title 15 U.S.C. @ 1125(c)(1) provides the following:

The owner of a famous mark shall be entitled, subject to the principles of equity and upon such terms as the court deems reasonable, to an injunction against another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become and causes dilution of the distinctive quality of the mark, and to obtain such other relief as is provided in this subsection.

Id. The section provides factors the court may consider in determining whether a mark is distinctive and famous. See 15 U.S.C. @ 1125(c)(1)(A-H). Though PEI's marks are arguably famous, their distinctiveness does not preclude defendant from the fair use of those items.

Under the Federal Trademark Dilution Act, a dilution claim is not actionable if there is a "fair use of a famous mark by another person in comparative commercial advertising or promotion to identify the competing goods or services of the owner of the famous mark." 15 U.S.C. @ 1125(c)(4)(A). As the court has indicated, Ms. Welles' use of the terms Playmate and [**22] Playmate of

the Year constitute identification of herself. The use of those terms, in the [illegible]site and in the meta tags, allows websurfers and potential customers to identify her services, whether it be her line of cigars, her promotional services, or her nude photographs. Given that Ms. Welles is the "Playmate of the Year 1981," there is no other way that Ms. Welles can identify or describe herself and her services without venturing into absurd descriptive phrases. In cases where the trademarked term must be used to identify the individual or a good, infringement and dilution laws do not apply. See New Kids, 971 F.2d at 306 ("In such cases, use of the trademark does not imply sponsorship or endorsement of the product because the mark is used only to describe the thing, rather than to identify its source."). Accordingly, plaintiff has failed to show that there is a likelihood of success on the merits of its dilution claim.

IV. CONCLUSION

In Prestonettes v. Coty, 264 U.S. 359, 368, 68 L. Ed. 731, 44 S. Ct. 350 (1924), Justice Holmes explained the purpose of trademark protection and noted that "when the mark is used in a way that does not deceive the public [**23] we see no such sanctity in the word as to prevent its being used to tell the truth. It is not taboo." In this case, Ms. Welles has used PEI's trademarks to identify herself truthfully as the "Playmate of the Year 1981." Such use is not "taboo" under the law. Based on the foregoing analysis, the court finds that plaintiff has failed to demonstrate that a preliminary injunction is warranted since there is not a strong likelihood of success on the merits. Consequently, the court cannot find that the balance of harm tips strongly enough in plaintiff's favor to overcome the lack of meritoriousness the court has found. See Stokely-Van Camp Inc. v. Coca-Cola Co., 1987 U.S. Dist. LEXIS 781, 2 U.S.P.Q.2D (BNA) 1225, 1227 (N.D. Ill. 1987). In addition, it is unclear that [illegible]eparable harm would ensue from the continued operation of Ms. Welles' website since plaintiff has not demonstrated that there is a likelihood of confusion. As such, the court, hereby, DENIES plaintiff's Motion for a Preliminary Injunction.

IT IS SO ORDERED.

5.20.98

Date

Judge Judith N. Keep

United States District Court

Southern District of California

BNA | TOP STORY | LIBRARY | FEEDBACK | SALES INFO

THE BUREAU OF NATIONAL AFFAIRS INC.

ELECTRONIC COMMERCE & LAW REPORT

MARKING 50 YEARS OF EMPLOYEE OWNERSHIP

Updated: 12/02/97 02:45 PM Eastern Standard Time

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

LOCKHEED MARTIN CORPORATION,
Plaintiff,
v.
NETWORK SOLUTIONS, INC., and DOES 1-20,
Defendants.

Case No. CV 96-7438 DDP (ANx)

Order Granting Defendant's Motion for Summary Judgment

The motion by defendant Network Solutions, Inc. ("NSI") for summary judgment came before the Court on October 6, 1997. After reviewing and considering the materials submitted by the parties and hearing oral argument, the Court grants the motion in its entirety.

I. Background

The issue presented by this litigation is whether NSI violated federal trademark law by accepting registrations of Internet domain names that are identical or similar to Lockheed Martin Corporation's ("Lockheed") SKUNK WORKS service mark. Lockheed asserts that NSI directly infringed and diluted its mark by accepting the registrations. Lockheed also asserts that NSI is liable as a contributory infringer because NSI did not comply with Lockheed's demands to cancel the registrations.

As to direct infringement, the Court concludes that NSI has not used Lockheed's service mark in connection with the sale, offering for sale, distribution or advertising of goods or service, and therefore cannot be liable for infringement under 15 U.S.C. §1114(1)(a) or for unfair competition under 15 U.S.C. §1125(a).

As to dilution, the Court finds that NSI has not made a commercial use of domain names as trademarks, and therefore cannot satisfy the commercial use element of dilution under 15 U.S.C. §1125(c).

As to contributory infringement, there are two potential bases for liability. First, a defendant is liable if it intentionally induced others to infringe a mark. **Inwood Labs., Inc. v. Ives Labs., Inc.**, 456 U.S. 844, 853-54, 102 S.Ct. 2182, 2188 (1982); **Fonovisa, Inc. v. Cherry Auction, Inc.**, 76 F.3d 259, 264 (9th Cir. 1996). Second, a defendant is liable if it continued to supply a product to others when the defendant knew or had reason to know that the party receiving the product used it to infringe a mark. **Inwood**, 456 U.S. at 853-54, 102 S.Ct. at 2488; **Fonovisa**, 76 F.3d at 264.

Lockheed has not presented evidence that NSI induced others to infringe Lockheed's service mark. Therefore, NSI is not liable under the first basis.

As to the knowledge basis, the Court concludes that NSI's limited role as a registrar of domain names coupled with the inherent uncertainty in defining the scope of intellectual property rights in a trademark militates against finding that NSI knew or had reason to know of potentially infringing uses by others. Furthermore, contributory infringement doctrine does not impose upon NSI an affirmative duty to seek out potentially infringing uses of domain names by registrants.

A. The Parties

For over 50 years, plaintiff Lockheed and its predecessors have operated "Skunk Works," an aerospace development and production facility. Lockheed owns the federally registered "SKUNK WORKS" service mark.

Defendant NSI is a publicly traded corporation with its principal place of business in Herndon, Virginia. Under a contract with the National Science Foundation, NSI is the exclusive registrar of most Internet domain names.

B. The Internet

The Internet is an international "super-network" connecting millions of individual computer networks and computers. The Internet is not a single entity. It is a highly diffuse and complex system over which no entity has authority or control. **See generally American Civil Liberties Union of Georgia v. Reno**, 929 F.Supp. 224, 930-45 (E.D. Pa. 1995), **aff'd**, 117 S.Ct. 2325 (1997). Although the Internet is now widely known for one of its ways of presenting information -- the World Wide Web ("Web") -- the Internet supports many other forms of communication. The Internet allows one-to-one communication via electronic mail ("e-mail"). In addition, one person can reach many other users through bulletin board services, newsgroups and numerous other Internet based means of communication. **Id.** at 834. All of these forms of Internet communication depend on the use of domain names to locate specific computers and networks on the Internet.

For commercial users, the Web is the most important part of the Internet. Unlike previous Internet-based communications formats, the Web is easy to use for people inexperienced with computers. Information on the Web can be presented on "pages" of graphics and text that contain "links" to other pages either within the same set of data files ("Web site") or within data files located on other computer networks. Users access information on the Web using "browser" programs. Browser programs process information from Web sites and display the information using graphics, text, sound and animation. Because of these capabilities, the Web has become a popular medium for advertising and for direct consumer access to goods and services. At the same time, the Web, like the rest of the Internet, is an important medium of non-commercial communications. The Web has made it easier for individuals and small organizations to publish information to the general public. Publication on the Web simply requires placing a formatted file on a host computer.

Web standards are sophisticated and flexible enough that they have grown to meet the publishing needs of many large corporations, banks, brokerage houses, newspapers and magazines which now publish "online" editions of their material, as well as government agencies, and even courts, which use the Web to disseminate information to the public. At the same time, Web publishing is simple enough that thousands of individual users and small community organizations are using the Web to publish their own personal "home pages," the equivalent of individualized newsletters about that person or organization, which are available to everyone on the Web.

Id. at 837. Much of the Web's usefulness derives from its use of links. A link is an image or a short section of text referring to another document on the Web. A user interested in accessing the referenced document selects the link, causing the document to be displayed automatically, along with a new set of links that the user may follow. **Id.** at 836.

While the linked structure of the Web is well-suited to allow users to browse among many sites, following whatever links happen to draw their interest, it is poorly suited for users who want to find a single Web site directly. Users searching for a specific Web site have two options. First, if users know or

can deduce the address of a Web site, they can type the address into a browser and connect directly to the Web site as if dialing a telephone number. **Panavision Int'l, L.P. v. Toeppen**, 945 F.Supp. 1296, 1299 (C.D. Cal. 1996). More often, users do not know the exact address and must rely on "search engines" available on the Web to search for key words and phrases associated with the desired Web site. Because of the quantity of information on the Web, searches often yield thousands of possible Web sites. Such a cumbersome process is rarely satisfactory to businesses seeking to use the Web as a marketing tool. Instead, businesses would prefer that customers simply be able to find a Web site directly using a corporate name, trademark or servicemark. **Panavision**, 945 F.Supp. at 1299.

1. The Domain Name System

Web sites, like other information resources on the Internet, are currently addressed using the Internet "domain name system." A numbering system called the "Internet Protocol" gives each individual computer or network a unique numerical address on the Internet. The "Internet Protocol number," also known as an "IP number," consists of four groups of digits separated by periods, such as "192.215.247.50." For the convenience of users, individual resources on the Internet are also given names. Specialized computers known as "domain name servers" maintain tables linking domain names to IP numbers.

Domain names are arranged so that reading from right to left, each part of the name points to a more localized area of the Internet. For example, in the domain name "cacd.uscourts.gov," "gov" is the top-level domain, reserved for all networks associated with the federal government. The "uscourts" part specifies a second-level domain, a set of the networks used by the federal courts. The "cacd" part specifies a sub-network or computer used by the United States District Court for the Central District of California.

If a user knows or can deduce the domain name associated with a Web site, the user can directly access the Web site by typing the domain name into a Web browser, without having to conduct a time-consuming search. Because most businesses with a presence on the Internet use the ".com" top-level domain name, as in "acme.com." Second-level domain names, the name just to the left of ".com," must be exclusive. Therefore, although two companies can have non-exclusive trademark rights in a name, only one company can have a second-level domain name that corresponds to its trademark. [1] For example, Juno Lighting, a maker of lamps, sought to establish a Web site with the address "juno.com," a domain name already in use by Juno Online Services, which uses the domain name as part of e-mail addresses for hundreds of thousands of e-mail customers. **See Juno Online Servs., L.P. v. Juno Lighting, Inc.**, ____ F.Supp. ____, 1997 WL 613021 (N.D. Ill. Sept. 29, 1997). In short, the exclusive quality of second-level domain names has set trademark owners against each other in the struggle to establish a commerical presence on the Internet, and has set businesses against domain name holders who seek to continue the traditional use of the Internet as a non-commercial medium of communication.

2. NSI's Role in the Domain Naming System

Under a contract with the National Science Foundation, NSI manages domain name registrations for the ".com," ".net," ".org," ".edu," and ".gov" top-level domains. The contract authorizes NSI to charge $100 for an initial two-year registration and $50 annually starting the third year. NSI registers approximately 100,000 Internet domain names per month. (Graves Decl. ¶ 5.) Registration applications are made via e-mail and in more than 90% of registrations no human intervention takes place. (Graves Depo. at 54.) On average, a new registration occurs approximately once every 20 seconds. (**Id.** at 47-48.)

NSI performs two functions in the domain name system. First, it screens domain name applications against its registry to prevent repeated registrations of the same name. Second, it maintains a directory linking domain names with the IP numbers of domain name servers. The domain name servers, which are outside of NSI's control, connect domain names with Internet resources such as Web sites and e-mail systems.

NSI does not make an independent determination of an applicant's right to use a domain name. Nor does

NSI assign domain names; users may choose any available second-level domain name. In 1995, NSI responded to the problem of conflicting claims to domain names by instituting a domain name dispute policy. Under the current policy, in effect since September 9, 1996, NSI requires applicants to represent and warrant that their use of a particular domain name does not interfere with the intellectual property rights of third parties. (Graves Decl. Ex. 1.) Under the policy, if a trademark holder presents NSI with a United States Patent and Trademark Office registration of a trademark identical to a currently registered domain name, NSI will require the domain name holder to prove that it has a pre-existing right to use the name. If the domain name holder fails to do so, NSI will cancel the registration. **(Id.)** NSI's policy has been criticized as favoring trademark owners over domain name holders, and favoring owners of federally registered marks over owners of non-registered marks, because owners of federally registered marks can invoke NSI's policy to effectively enjoin the use of identical domain names without having to make any showing of infringement or dilution. Jerome Gilson & Jeffrey M. Samuels, **Trademark Protection and Practice**, §§5.11[4][B], at 5-239, 5.11[5], at 5-243 (1997) (noting that NSI's policy is tilted in favor of trademark owners, who can deprive registrants of domain names without meeting the likelihood of confusion test for infringement or showing that the domain name dilutes the mark); Gayle Weiswasser, **Domain Names, the Internet, and Trademarks Infringement in Cyberspace**, 13 **Santa Clara Computer & High Tech. L. J.** 137, 172-73 (1997). If a trademark holder and domain name registrant take their dispute to court, NSI will deposit the domain name in the registry of the court. This process maintains the status quo; the domain name remains active while in the registry of the court. [2]

C. Factual Background

Most of the underlying facts of this case are not in dispute. The dispute at summary judgment is over the interpretation of the law and the application of the law to the facts. The court finds that there is no genuine issue as to the following facts:

1. Lockheed owns the federally registered SKUNK WORKS service mark for "engineering, technical consulting, and advisory services with respect to designing, building, equipping, and testing commercial and military aircraft and related equipment." (Land Decl. Exs. A & B (Certificate of Registration Nos. 968,861 & 1,161,482).)

2. In August 1994, Seng-Poh Lee registered the domain name "skunkwrks.com" with NSI. Lee did not associate the domain name with a web site. In March 1996, Lockheed demanded that Lee cancel his registration. In May 1996, Lee complied. However, Lockheed did not apply to NSI for registration of the name. It became generally available and was registered by Grant Smith, a resident of the United Kingdom, in December 1996. (Graves Decl. ¶ 14; Quinto Decl. Ex. H.)

3. In September 1995, Kathy Huber, a resident of New York, registered "skunkworks.com" with NSI for the use of her employer Skunkworks Marketing Lab, Inc ("SML"). SML used the domain name for e-mail only; it did not associate a web site with the domain name. (Jones Decl. Ex. 4.) On March 21, 1996, Lockheed sent a cease-and-desist-letter to SML. (Meeg Decl. Ex. C.) SML filed a petition in the United Sates Patent and Trademark Office seeking to cancel registration of the SKUNK WORKS mark on the grounds that "skunk works" was generic. SML has since moved to withdraw its petition. (Quinto Decl. ¶¶ 9-11.)

4. In January 1996, Ken Hoang, a resident of California, registered the domain name "skunkwrks.com" with NSI for use by his company Skunk Works Multimedia, Inc. Lockheed sued Hoang's company for trademark infringement in May 1996. **Lockheed Martin Corp. v. Clayton Jacobs**, CV 96-3422 (C.D. Ca. filed May 13, 1996). On July 23, 1996, that action resulted in a consent judgment under which the parties agreed that the domain name would be assigned to Lockheed. (Jones Decl. Ex. 7.) Lockheed claims that it provided NSI with a file-stamped copy of the consent judgment and requested that NSI transfer the infringing domain name registrations to Lockheed, but NSI took no action. (Quinto Decl. ¶¶ 6, 7.) NSI, however, asserts that Lockheed has failed to complete the necessary form to effect the transfer despite offers of assistance by NSI's counsel. (Heeg Decl. ¶ 2, Ex. A.).

5. In January 1996, Roger Barski, an Illinois resident, registered the domain name "skunkwerks.com" with NSI. Barski used the domain name in association with a Web site offering his services as a Web

site designer. (Jones Decl. Ex. 5.) After receiving a cease-and-desist letter from Lockheed, Barski canceled his "skunkwerks.com" account with his Internet service provider, essentially deactivating the domain name. He did not, however, request to have the name removed from NSI's registry.

6. On May 7, 1996 Lockheed sent NSI a letter advising NSI that Lockheed owned the SKUNK WORKS mark and requesting that NSI cease registering domain names that referred to or included the names "skunk works" or "skunkworks" or otherwise infringed Lockheed's mark. (Quinto Decl. Ex. A.) Lockheed also requested that NSI provide Lockheed with a list of registered domain names that contain the words "skunk works" or any variation thereof. Lockheed's letter did not include a certified copy of its trademark registration. (**Id.**; Graves Decl. ¶ 11.)

7. On June 18, 1996, Lockheed sent a second letter, informing NSI that the registrant of "skunkworks.com" had agreed to stop using the domain name, and that the registrant of "skunkworks.net" was being sued in federal district court. (Quinto Decl. Ex. C.) The letter did not refer to the lawsuit by docket number or caption, nor did it include a copy of the complaint or other pleading. (**Id.**)

8. In September 1996, James McBride, a Missouri resident, acting as the administrative contact for Skunkworx Industries, Ltd, registered the domain name "skunkworx.com" with NSI. (Quinto Decl. Ex. K.) The parties have not presented evidence of use of this domain name in connection with Web sites or other forms of communication.

9. On September 18, 1996, NSI's Internet business manager, David Graves, wrote to Lockheed's counsel in response to the May 7 and June 18 letters. NSI informed Lockheed that NSI could not provide a list of all domain names that included "skunkworks" or any variation thereof, but that Lockheed could use the public "Whois" database of domain name registrations to find this information. NSI further informed Lockheed that upon receipt of a file-stamped copy of the complaint in the "skunkworks .net" case, NSI would immediately deposit the domain name in the registry of the court, maintaining the status quo until the court ordered otherwise. (Graves Decl. Ex. 5.)

10. In December 1996, Terry Robinson, a Texas resident, registered the domain name "the-skunkwerks .com" with NSI. (Quinto Dec. Ex. L.) The parties have not presented evidence of use of this domain name in connection with Web sites or other forms of communication.

11. On January 3, 1997, Peter Pasho, a resident of Canada, registered the domain name "theskunkworks.com" with NSI. (Quinto Dec. Ex. M.) Pasho has associated the domain name with a Web site offering his services as a Web site designer. (Quito Decl. Ex. N.) As of April 9, 1997, this Web site included a page depicting a Lockheed-designed aircraft and briefly discussing its design at the Lockheed Skunk Works. (**Id.**)

D. Procedural Background

Lockheed filed this action on October 22, 1996, alleging infringement, unfair competition, dilution and contributory infringement under the Lanham Act, and seeking injunctive and declaratory relief. NSI answered the complaint and counterclaimed for declaratory relief.

On March 19, 1997, this Court denied NSI's motion to dismiss for failure to join the domain name registrants as indispensable parties under Federal Rule of Civil Procedure 19(b). **Lockheed Martin Corp. v. Network Solutions, Inc.**, 43 U.S.P.Q.2d 1056 (C.D. Cal. 1997).

On September 29, 1997, this Court denied Lockheed's motion to file a first amended complaint adding a cause of action for "contributory dilution." The Court denied the motion on the bases of futility, undue delay and prejudice.

NSI's present motion seeks summary judgment on all of Lockheed's claims.

II. Discussion

This Court has subject matter jurisdiction over Lanham Act claims pursuant to 28 U.S.C. §§1331 and 1338(a). NSI has consented to personal jurisdiction by appearing in this action. Fed.R.Civ.P. 12(h)(1).

A. Standard for Summary Judgment

Summary judgment is appropriate when there is no genuine issue of material fact and the moving party is entitled to a judgment as a matter of law. Fed.R.Civ.P. 56(c), **see Celotex Corp. v. Catrett**, 477 U.S. 317, 106 S.Ct. 2548 (1986).

In order to defeat a motion for summary judgment, there must be facts in dispute that are both genuine and material, i.e., there must be facts upon which a fact finder could reasonably find for the non-moving party. **See Anderson v. Liberty Lobby, Inc.**, 477 U.S. 242, 252 106 S.Ct. 2505, 2515 (1986). The Court does not weigh the evidence or make credibility determinations; rather, the court only determines whether there are any disputed issues and, if so, whether those issues are both genuine and material. **Id.**

The initial burden of establishing that there is no genuine issue of material fact lies with the moving party. Fed.R.Civ.P. 56(c); **Celotex**, 477 U.S. at 323, 106 S.Ct. at 2552-53; **British Airways Board v. Boeing Co.**, 585 F.2d 946, 951 (9th Cir. 1978). Once the movant has met this burden by procuring evidence that, if left uncontroverted, would entitle the moving party to a direct verdict at trial, the burden shifts to the non-movant to present specific facts showing that there is a genuine issue of material fact. **See** Fed.R.Civ.P. 56(e); **Celotex** 477 U.S. at 324, 106 S.Ct. at 2553; **Lake Nacimiento Ranch Co. v. San Luis Obispo**, 841 F.2d 872, 876 (9th Cir. 1997).

Summary judgment is disfavored in trademark cases because of the inherently factual nature of most trademark disputes. **See Levi Strauss & Co. v. Blue Bell, Inc.**, 778 F.2d 1352, 1355 (9th Cir. 1985). Nonetheless, summary judgment is appropriate "where the party opposing the motion fails to demonstrate the existence of any material issues of fact for trial." **Sykes Laboratory, Inc. v. Kalvin**, 610 F.Supp. 849, 860 (C.D. Cal. 1985).

B. Trademark Infringement Under Lanham Act Section 32, 15 U.S.C. §1114(1)

Section 32 of the Lanham Act prohibits a person from using another's mark without permission "in connection with the sale, offering for sale, distribution or adertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive ... ." 15 U.S.C. §1114(1). To be liable under section 32, a person must use the mark on competing or related goods in a way that creates a likelihood of confusion. **AMF Inc. v. Sleekcraft Boats**, 599 F.2d 341, 348 (9th Cir. 1979). Before considering the likelihood of confusion, however, the Court must determine whether NSI, by accepting registrations, has used the SKUNK WORKS mark in connection with the sale, distribution or advertising of goods or services. **See Planned Parenthood Fed'n of America, Inc. v. Bucci**, 42 U.S.P.Q.2d 1430, 1434 (S.D.N.Y. 1997).

Domain names present a special problem under the Lanham Act because they are used for both a non-trademark technical purpose, to designate a set of computers on the Internet, and for trademark purposes, to identify an Internet user who offers goods or services on the Internet. **See** 2 Gilson, **supra**, §5.11(3), at S-235, 5.11(5), at S-243-44 (distinguishing the technical use of domain names from the trademark use to identify goods or services). When a domain name is used only to indicate an address on the Internet, the domain name is not functioning as a trademark. [3] **See Walt-West Enters., Inc. v. Gannett Co., Inc.**, 695 F.2d 1050, 1059-60 (7th Cir. 1982) (radio station frequency used in "utilitarian sense of calling the listener's attention to a location on the FM dial" is not protectable under trademark law). Like trade names, domain names can function as trademarks, and therefore can be used to infringe trademark rights. **See Accuride Int'l, Inc. v. Accuride Corp.**, 671 F.2d 1531 (9th Cir. 1989). Domain names like trade names, do not act as trademarks when they are used merely to identify a business entity; in order to infringe they must be used to identify the source of goods or services. **Cf. In re Unclaimed Salvage & Freight Co.**, 192 U.S.P.Q. 165, 168 (T.T.A.B. 1976) (affirming refusal of registration of trade name as trademark where specimen demonstrated use only to identify applicant as a business); U.S. Dept. of Commerce, Patent and Trademark Office, Trademark Manual of Examining

Procedure §1202.02, at 1202-3 (2d ed. May 1993) (directing examiners to refuse registration of material that functions only to identify a business.)

NSI's acceptance of domain name registrations is connected only with the name's technical function on the Internet to designate a set of computers. By accepting registrations of domain names containing the words "skunk works," NSI is not using the SKUNK WORKS mark in connection with the sale, distribution or advertising of good and services. NSI merely uses domain names to designate host computers on the Internet. This is the type of purely "nominative" function that is not prohibited by trademark law. **See New Kids on the Block v. New America Pub., Inc.**, 971 F.2d 302, 307 (9th Cir. 1992) (noting that laws against infringement do not apply to "non-trademark use of a mark") **Lucasfilm, Ltd. v. High Frontier**, 622 F.Supp. 931, 933 (D.D.C. 1985) (holding that property rights in a trademark do not extend to the use of the trademark to express ideas unconnected with the sale or offer for sale of goods or services).

This is not to say that a domain name can never be used to infringe a trademark. However, something more than the registration of the name is required before the use of a domain name is infringing. In **Planned Parenthood Fed'n of America, Inc. v. Bucci**, for example, the defendant registered the domain name "plannedparenthood.com" and used it as the address of a Web site promoting his book on abortion. 42 U.S.P.Q.2d 1430, 1432 (S.D.N.Y. 1997). The defendant admitted that he used the domain name hoping that people looking for the Planned Parenthood site would find this site. **Id.** at 1433. The defendant argued that registration without more is not a commercial use of a mark. **Id.** at 1436. The court, however, found that the defendant did "more than merely register a domain name; he has created a home page that uses plaintiff's mark as its address, conveying the impression to Internet users that plaintiff is the sponor of defendant's web site." **Id.** at 1437. The infringing use in **Planned Parenthood** was not registration of the plaintiff's mark with NSI, but rather the use of the plaintiff's trademark "as a domain name to identify his web site" in a manner that confused Internet users as to the source or sponsorship of the product offered there. **Id.** at 1440; **cf. TeleTech Customer Care Management (California), Inc. v. TeleTech Co.**, 42 U.S.P.Q.2d 1913, 1919 (C.D. Cal. 1997) (finding that the plaintiff was not likely to prevail on the merits of an infringement claim because the plaintiff demonstrated only that customers were likely to be confused as to location of Web site, not as to source of goods or services).

The cases dealing with vanity telephone numbers are consistent with the conclusion that registration of a domain name, without more, does not constitute use of the name as a trademark. A toll-free telephone number with an easy-to-remember letter equivalent is a valuable business asset. As with domain names, courts have held that the promotion of a confusingly similar telephone number may be enjoined as trademark infringement and unfair competition. **Dial-a-Mattress Franchise Corp. v. Page**, 880 F.2d 675, 678 (2d Cir. 1989); **American Airlines, Inc. v. A 1-800-A-M-E-R-I-C-A-N Corp.**, 622 F. Supp. 673 (N.D. Ill. 1985). The infringing act, however, is not the mere possession and use of the telephone number. If it were, trademark holders would be able to eliminate every toll-free number whose letter equivalent happen to correspond to a trademark. In **Holiday Inns, Inc. v. 800 Reservation, Inc.**, 86 F.3d 619 (6th Cir. 1996), the district court held that the defendant's use of 1-800 H[zero]LIDAY infringed the plaintiff's trademark in the telephone number 1-800-HOLIDAY. **Id.** at 620. The court of appeals reversed, holding that Holiday Inn's trademark rights in its vanity telephone number did not allow it to control use by others of confusingly similar telephone numbers. Although the defendant's toll-free number was often misdialed by customers seeking 1-800-HOLIDAY, the defendant never promoted the number in connection with the HOLIDAY trademark; but only prompted it as 1-800-405-4329. **Id.** at 623. Because the defendant had used the number only as a telephone number, and not as a trademark the court of appeals held that the defendant had not infringed the plaintiff's trademark. **Id.** at 625-26.

Domain names and vanity telephone numbers both have dual functions. Domain names, like telephone numbers, allow one machine to connect to another machine. Domain names, like telephone numbers, are also valuable to trademark holders when they make it easier for customers to find the trademark holder. Where the holder of a vanity telephone number promotes it in a way that causes a likelihood of confusion, the holder has engaged in an infringing use. **American Airlines**, 622 F. Supp. at 682 (mere use of telephone number is not infringing, but misleading use of trademarked term in yellow pages

advertisement is infringing). But, where, as with NSI, the pure machine-linking function is the only use at issue, there is no trademark use and there can be no infringement.

In the ordinary trademark infringement case, where there is no question that the defendant used the mark, the analysis proceeds directly to the issue of whether there is a likelihood of confusion. Here, however, because NSI has not used Lockheed's service mark in connection with goods or services, the Court need not apply the test for likelihood of confusion. NSI, therefore, is entitled to judgment as a matter of law on the section 32 claim.

1. Printer and Publisher Liability Under 15 U.S.C. §1114(2)(A), (B)

Lockheed asserts that NSI has infringed its service mark as a "printer" of the mark under 15 U.S.C. §1114(2)(A). This assertion misapprehends NSI's function as a domain name registrar. To the extent that registrants of SKUNK WORKS-type domain names infringed the mark, they did so by using it on Web sites or other Internet resources in a way that created a likelihood of confusion as to source or sponsorship. NSI is not an Internet service provider. It does not provide host computers for Web sites on other Internet resources. NSI's role is restricted to publishing a list of domain names, their holders, and the IP numbers of the domain name servers that perform the directory function associated with the domain names. (Graves Decl. ¶ 10.) ISP liability?

NSI's role is fundamentally dissimilar from that of telephone directory publishers whose conduct has been found enjoinable under §1114(2)(A). **See Century 21 Real Estate Corp. of Northern Illinois v. R.M. Post Inc.**, 8 U.S.P.Q.2d 1614, 1617 (N.D. Ill. 1988) (denying motion to dismiss where yellow pages publishers were alleged to have printed infringing trademark in listing of former licensee who no longer had right to use trademark). There, the telephone directory printers supplied the material that directly caused the likelihood of confusion. In the domain name context, the domain name registration itself does not infringe the trademark. Infringement occurs when the domain name is used in certain ways. For example, a domain name may infringe trademark rights when it is used in connection with a Web site that advertises services in competition with those of the trademark owner. **See, e.g., Cardservice International, Inc. v. McGee**, 950 F.Supp. 737, 738 (E.D. Va. 1997); **Comp Examiner Agency, Inc. v. Juris, Inc.**, 1996 WL 376600 (C.D. Cal. 1996). Where domain names are used to infringe, the infringement does not result from NSI's publication of the domain name list, but from the registrant's use of the name of a Web site or other Internet form of communication in connection with goods or services. NSI is not a "printer or publisher" of Web sites, or any other form of Internet "publication." As discussed below in the section on contributory infringement, NSI's involvement with the use of domain names does not extent beyond registration. NSI's liability cannot be premised on an argument that it prints or publishers the list of domain names, because the list is not the instrument or forum for infringement. NSI's liability, if it exists at all, would stem from registrants' use of domain names in connection with other services not provided by NSI. This type of liability is properly analyzed under contributory liability doctrine, not as printer and publisher liability under §1114(2)(A).

C. Unfair Competition Under Lanham Act Section 43(a), 15 U.S.C. §1125(a)

Lockheed has followed the common practice of alleging unfair competition under section 43(a) of the Lanham Act along with trademark infringement under section 32. Both causes of action depend on a demonstration of a likelihood of confusion. 1 J. Thomas McCarthy, **McCarthy on Trademarks and Unfair Competition** §2:8 (1997). Federal unfair competition requires use of the mark in connection with goods or services, 15 U.S.C. § 1125(a)(1). As discussed above, NSI's acceptance of registrations for domain names resembling SKUNK WORKS is not a use of the mark in connection with goods or services.

A recent district court decision illustrates the application of federal unfair competition law to the domain name context. **Juno Online Servs., L.P. v. Juno Lighting, Inc.**, __ F.Supp. __, 1997 WL 613021 (N.D. Ill. Sept. 29, 1997). During a dispute over the domain name "juno. com," Juno Lighting registered the domain name "juno-online.com" in the hopes of persuading Juno Online Services to switch its e-mail service to that domain name. Juno Online sued Juno Lighting for federal unfair competition. The district court dismissed the unfair competition claim because Juno Online alleged only that Juno Lighting

registered the name with NSI, and did not allege further use of the name to create a Web site or to advertise its services. **Id.** at *8-*9. The court held that registration of a trademark as a domain name does not constitute use of the trademark on the Internet in connection with goods or services, and therefore was not prohibited by action 43(a). **Id.** This reasoning applies more strongly to NSI which has not registered domain names resembling SKUNK WORKS for its own use, but has merely accepted domain name registrations from others.

D. Trademark Dilution Under the Federal Trademark Dilution Act of 1995, Lanham Act Section 43(c), 15 U.S.C. §1125(c)

Trademark dilution laws protect "famous" marks from certain unauthorized uses regardless of a showing of competition, relatedness or likelihood of confusion. The federal dilution statute entitles the owner of a famous mark to enjoin "another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark ... " 15 U.S.C. §1125(c)(1). Dilution is defined as "the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of -- (1) competition between the owner of the famous mark and other parties, or (2) likelihood of confusion, mistake or deception." 15 U.S.C. §1127. The Federal Trademark Dilution Act specifically excludes non-commercial use of a mark from its coverage. 15 U.S.C. §1125(c)(4)(B).

NSI's acceptance of domain name registrations is not a "commercial use" within the meaning of the Federal Trademark Dilution Act. Lockheed argues that NSI engages in commercial use because the registration of SKUNK WORKS-type domain names inhibits Lockheed's ability to use its service mark as a domain name. (Opp'n at 29.) Lockheed contends that NSI's conduct is similar to that of the defendant in **Panavision Int'l L.P. v. Toeppen**, 945 F.Supp. 1296, 1299 (C.D. Cal. 1996). In **Panavision** the defendant, Teoppen, was a "cybersquatter," an entrepreneur who made a business of registering trademarks as domain names for the purpose of selling them later to the trademarks' owners. **Panavision**, 945 F Supp. at 1303. The court held that Toeppen "traded on the value of the marks as marks by attempting to sell the domain names to Panavision." **Id.** The court found that "[t]his conduct injured Panavision by preventing Panavision from exploiting its marks and it injured customers because it would have been difficult to locate Panavision's web site if Panavision had established a web site under a name other than its own." **Id.**; **see also Intermatic Inc. v. Toeppen**, 947 F.Supp. 1227, 1239 (N.D. Ill. 1995) (holding that defendant's use of the mark was diluting because it prevented plaintiff from using it). Lockheed's argument implies that any conduct that makes it more difficult for Lockheed to establish a presence on the Internet is diluting conduct. This argument is flawed. In **Panavision** and **Intermatic**, the fact that the defendant's conduct impeded plaintiff's use of its trademark as a domain name was not the determining factor in finding that the defendant's use was diluting. If impeding use of the trademark as a domain name were the only factor, the court in **Panavision** would not have asserted that registration of a trademark "as a domain name, without more, is not a commercial use of the trademark and therefore not within the prohibitions of the Act." **Panavision**, 945 F.Supp. at 1303. All prior domain name registrations corresponding to words in a trademark impede the trademark owner's use of the same words for use as a domain name. The Internet, however, is not exclusively a medium of commerce. The non-commercial use of a domain name that impedes a trademark owner's use of that domain name does not constitute dilution. [4] In **Intermatic** and **Panavision**, the defendant's use was commercial because the defendant sought to "arbitrage" the trademarks for their value as domain names. **Intermatic**, 947 F.Supp. at 1239; **Panavision**, 945 F.Supp. at 1303. Lockheed argues that NSI is engaged in commercial use of its service mark because NSI seeks to maximize the number of domain names registered in order to maximize its revenue and profits. (Opp'n at 27.) Lockheed cites statements in NSI's Initial Public Offering registration statement ("IPO") [5] to the effect that part of NSI's strategy for growth is to stimulate demand for domain names in targeted customer segments, including among trademark owners. (**Id.**; **see** Rierson Decl. Ex. B.) Lockheed contends that like Toeppen, NSI trades on the value of domain names by "selling" registrations to as many people as possible. (**Id.**) NSI, however, does not trade on the value of domain names as trademarks. NSI's use of domain names is connected to the names' technical function on the Internet to designate computer addresses, not to the names' trademark function to distinguish goods and services. The fact that NSI makes a profit from the technical

function of domain names does not convert NSI's activity to trademark use. **See New Kids**, 971 F.2d at 309. The Court does not question that a domain name which is easily deducible from a trademark is a valuable asset to the trademark owner. Such a domain name makes it easier for the trademark owner's customers to find the trademark owner's Internet resources such as Web sites. But a domain name's correspondence to a trademark does not make the domain name any more valuable to NSI, whose only interest in a domain name is as a pointer to an IP number. NSI, unlike the defendant in **Intermatic** and **Panavision**, does not make a commercial use of domain names by trading on their value as trademarks.

Because the Court finds as a matter of law that NSI does not make commercial use of domain names as trademarks, Lockheed cannot prevail on its dilution claim. The Court therefore does not address the other dilution elements.

E. Contributory Infringement

Lockheed asserts that NSI is liable for contributory infringement of the SKUNK WORKS mark because NSI accepted registrations of domain names similar to the mark and refused to cancel the registrations in response to Lockheed's demands. Contributory infringement doctrine extends liability to reach manufacturers and distributors who do not themselves use the mark in connection with the sale of goods, but who induce such use by supplying goods to direct infringers. Liability for contributory infringement requires that the defendant either "(1) intentionally induces another to infringe on a trademark or (2) continues to supply a product knowing that the recipient is using the product to engage in trademark infringement." **Fonovisa, Inc. v. Cherry Auction, Inc.**, 76 F.3d 259, 264 (9th Cir. 1996) (citing the test set forth in **Inwood Laboratories, Inc. v. Ives Laboratories, Inc.**, 456 U.S. 844, 853-54, 102 S. Ct. 2182, 2188 (1982)). Lockheed does not contend that NSI induced infringement. No evidence has been presented to indicate inducement. The issue, therefore, is whether Lockheed has created a genuine issue as to the knowledge prong of the **Inwood** test.

Following **Inwood**, courts have extended liability for trademark infringement beyond direct infringers, but only under certain circumstances. **Mini Maid Servs. Co. v. Maid Brigade Sys., Inc.**, 967 F.2d 1516, 1521 (11th Cir. 1992). The clearest circumstances for extending liability are those presented by **Inwood** itself. There, a pharmaceutical manufacturer supplied generic drugs that some pharmacists mislabled as brand-name drugs. Each extension of contributory liability doctrine beyond defendants who manufacture or distribute a mislabeled product has required careful examination of the circumstances to determine whether knowledge of infringement should be imputed to the alleged contributory infringer. **See Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc.**, 955 F.2d 1143, 1148 (7th Cir. 1992) (holding that the landlord/tenant relationship between a flea market operator and vendors provides a basis for extending contributory trademark infringement doctrine in circumstances indicating willful blindness of the flea market operator toward the vendors' blatantly infringing acts); **Fonovisa**, 76 F.3d at 265 (same) **Mini Maid**, 967 F.2d at 1522 (extending contributory liability doctrine to a franchisor/franchisee relationship but holding that the district court erred in finding contributory liability based on the franchisor's failure to supervise the franchisee with reasonable diligence). Lockheed now asks that the Court extend contributory liability to the relationship between a domain name registrar and domain name registrants who are alleged to have directly infringed Lockheed's mark.

NSI is involved only in the registration of domain names, not in the use of domain names in connection with goods and services on the Internet. (Graves Decl. ¶ 10); **cf, Intermatic**, 947 F.Supp at 1231-32 (noting that there is no technical connection between domain name service and contents of Web sites or other Internet resources). NSI does not provide the other services needed to use the domain name in association with a Web site or other means of communication on the Internet. The services necessary to maintain a Web site, such as an IP address, communications, computer processing and storage are performed by Internet service providers ("ISP") who provide the host computers and connections necessary for communications on the Internet. It is not necessary to secure a second-level domain name registration in order to establish a presence on the Internet. Users may simply use the second-level domain name of the ISP. Where domain name registration is necessary, the ISP usually acts as an agent to secure and maintain the registration. **See Domain Name System, Hearings Before the Subcomm. on Basic Research of the House Science Comm.**, 105th Cong., 1997 WL 14151463 (September 30, 1997) (testimony of Barbara A. Dooley, Executive Director, Commercial Internet Exchange

ISP liability?

Association) (noting that most users rely on ISPs to act as agents to secure and maintain registrations, and that ISPs are the primary providers with a close relationship to end users).

The registration of a domain name, without more, does not amount to infringement of a mark similar to the name. **Panavision**, 945 F.Supp. at 1303. Infringing acts occur when a domain name is used in a Web site or other Internet form of communication in connection with goods or services. **Planned Parenthood Fed'n of America v. Bucci**, 42 U.S.P.Q.2d 1430, 1437 (S.D.N.Y. 1997). After a domain name is registered, NSI's involvement is over. NSI is not part of the process of linking domain names with potentially infringing resources such as Web sites. NSI does not require holders to use domain names for Web sites or any other form of Internet communication. [6] Nor do domain name holders need NSI's permission to do so.

Because NSI's involvement with the Internet is remote from domain name uses that are capable of infringement, Lockheed's reliance on the flea market cases, **Fonovisa** and **Hard Rock**, is misplaced. In **Hard Rock**, the Seventh Circuit noted that the common law of landlord/tenant relations imposes vicarious liability on a landlord who knows or has reason to know of the tortious activity of those whom the landlord permits on the landlord's premises. **Hard Rock**, 955 F.2d at 1149. Because the landlord/tenant standard is similar to the **Inwood** standard for contributory infringement by manufacturers, the court held that the **Inwood** standard should apply to flea market operators who lease space to vendors. **Id.** This holding was further supported by the district court's finding that the flea market operator not only rented space, but also advertised and promoted the activity on its premises, sold tickets and directly supervised the premises. **Id.** at 1148. In **Fonovisa**, the Ninth Circuit adopted **Hard Rock's** analogy between landlord/tenant vicarious liability and trademark law contributory liability in order to extend the **Inwood** standard to the flea market context. **Fonovisa**, 76 F.3d at 265. There, too, the court found that the flea market operator provided more than space, and was directly and substantially involved in the businesses of the infringing vendors. **Id.** at 264.

The flea market operators directly controlled and monitored the premises. NSI neither controls nor monitors the Internet. A domain name, once registered, can be used in connection with thousands of pages of constantly changing information. While the landlord of a flea market might reasonably be expected to monitor the merchandise sold on his premises, NSI cannot reasonably be expected to monitor the Internet. **SeeAmerican Civil Liberties Union of Georgia v. Reno**, 929 F.Supp. 824, 832 (E.D. Pa. 1996), **aff'd**, 117 S.Ct. 2329 (1997) ("There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet."). NSI's role in the Internet is distinguishable from that of an Internet service provider whose computers provide the actual storage and communications for infringing material, and who therefore might be more accurately compared to the flea market vendors in **Fonovisa** and **Hard Rock.** [7] **See Religious Technology Center v. Netcom On-Line Communication Services, Inc.**, 907 F.Supp. 1361, 1373 (N.D. Cal. 1995).

Because NSI's involvement with potentially infringing uses of domain names is remote, the Court finds that it is inappropriate to extend contributory liability to NSI absent a showing that NSI had unequivocal knowledge that a domain name was being used to infringe a trademark.

1. NSI's Knowledge

The mere assertion by a trademark owner that a domain name infringes its mark is not sufficient to impute knowledge of infringement to NSI. The use of an identical or similar mark does not necessarily constitute infringement. In order to be infringing, such use must be in connection with goods or services that are competitive with, or at least related to, the goods or services for which the trademark has been registered or used in commerce. **AMF Inc. v. Sleekcraft Boats,** 599 F.2d 341, 348 (9th Cir. 1979). The use must also cause a likelihood of confusion as to origin or sponsorship. **Id.** Whether a use is likely to cause confusion depends on numerous variables including the strength of the mark, the proximity of the goods, the similarity of the marks, evidence of actual confusion, marketing channels used, the type of goods and degree of care used by purchasers, the defendant's intent in selecting the mark, and the likelihood of expansion of product lines. **Eclipse Associates Ltd. v. Data General Corp.,** 894 F.2d 1114, 1117 (9th Cir. 1990).

Why did it do this?

NSI's registration form requires the applicant to state the purpose of the domain name registration. Lockheed contends that NSI receives sufficient information on the form to know whether a domain name registration will be used to infringe a mark, and that the use of the form satisfies the knowledge element of contributory infringement doctrine. The form instructs the applicant to "[b]riefly describe the domain name Registrant and the purpose for which this domain name is being applied." (Quinto Decl. in Opp'n to Ex Parte Application for Order Finding Civil Contempt, Ex. C.) Infringement depends on likelihood of confusion. The likelihood of confusion test examines the totality of circumstances under which a mark is used. **See Eclipse,** 894 F.2d at 1118. The outcome of the test cannot be predicted from an examination of the mark and the domain name in connection with a brief statement of the purpose for which the mark is being used. A reasonable person in NSI's position could not presume infringement even where the domain name is identical to a mark and registered for use in connection with a similar or identical purpose. **See Taj Mahal Enterprises, Ltd. v. Trump,** 745 F.Supp. 240 (D.N.J. 1990) (finding insufficient likelihood of confusion between TAJ MAHAL mark as used by restaurant and TAJ MAHAL mark as used by casino and hotel complex which included several restaurants); **Church of the Larger Fellowship, Unitarian Universalist v. Conservation Law Foundation of New England, Inc.,** 221 U.S.P.Q. 869 (D. Mass 1983) (finding insufficient likelihood of confusion between plaintiff's use of CLF mark for direct mail charitable solicitation and defendant's use of CLF mark for same purpose in same city); **Pump, Inc. v. Collins Management, Inc.,** 746 F.Supp. 1150 (D. Mass. 1990) (granting defendant's motion for summary judgment, finding insufficient likelihood of confusion between plaintiff's use of PUMP for purpose of promoting rock band and defendant's use of PUMP for same purpose). The receipt of a brief statement of purpose from domain name applicants does not give NSI sufficient information for the Court to impute knowledge of future infringing uses to NSI.

An owner's rights in a trademark do not remain stable over time. The scope of the owner's rights is subject to contraction if the trademark is abandoned or becomes generic for all or part of the goods or services identified. This dynamic nature of trademark rights increases their inherent uncertainty. Lockheed concedes that the Lanham Act recognizes that a mark may become generic for a portion of the goods or services for which it is registered, causing the owner to lose trademark protection against use of the mark in connection with such goods. (Lockheed's Separate Statement of Genuine Issues at 11); 15 U.S.C. §1064 (providing for cancellation of trademark registration with respect to goods and services for which mark has become generic). NSI submits evidence of numerous third-party uses of the term "skunk works" to describe a type of corporate management style. (Jones Decl. Exs. 14-44.) (newspaper, magazine and trade journal articles describing "skunk works" at companies including IBM, Chrysler, General Motors, Buick, Compaq, Patagonia and Bell Atlantic). "Skunk works" is defined in the 1996 American Heritage Dictionary as "[a] small loosely structured corporate research and development unit or subsidiary formed to foster innovation."(Jones Decl. Ex. 9.) Parallel generic meanings do not remove trademark protection over uses of the trademarked term to distinguish the source of goods. 2 McCarthy §12:3. The trademark owner, however, does not have protection against purely generic or nominative uses of the term that do not serve to distinguish goods or services. [8] 15 U.S.C. §1064; **New Kids on the Block v. New America Pub. Inc.,** 971 F.2d 302 (9th Cir. 1992); **Lucasfilm Ltd. v. High Frontier,** 622 F.Supp. 931 (D.D.C. 1985). The existence of numerous legitimate, non-infringing uses of the term "skunk works" further illustrates the uncertainty inherent in the question of whether NSI knew or had reason to know of infringing uses of domain name registrations. [9]

Additionally, trademark law permits multiple parties to use and register the same mark for different classes of goods and services. NSI points to United States Trademark Registration 1,941,484 for SKUNKWORKS PUBLISHING for use on printed publications relating to business (Jones Decl. Ex. 45.) The applicant was required to disclaim any rights to PUBLISHING apart from the mark as shown. (**Id.** Ex. 46.) Where a party disclaims portions of the mark, the un-disclaimed portions are considered "dominant" for purposes of customer confusion. **In re Dixie Restaurants, Inc.,** 105 F.3d 1405, 1407 (Fed. Cir. 1997) (holding that there was a likelihood of confusion between THE DELTA CAFE and DELTA where the owner of the former trademark disclaimed CAFE). Therefore, for purposes of determining possible infringement by the domain name "skunkworks.com," SKUNK WORKS and SKUNKWORKS PUBLISHING are the same mark. If NSI had received letters from both Lockheed and the registered owner of SKUNKWORKS PUBLISHING, it would have no basis for deciding which party's rights placed NSI at greater risk of liability for contributory infringement. The proper course of

action in such a situation would be for NSI to initiate an interpleader action, placing the domain name in the registry of the court and allowing the claimants to adjudicate the question of whether one claimant's trademark rights allowed exclusive use of the mark as an Internet domain name. (**See** Grave Decl. Ex. 1 (domain name dispute policy).)

In holding that the degree of uncertainty over infringing uses of domain names makes it inppropriate to impose contributory liability on NSI, the Court is not making new trademark rules for the Internet. Contributory infringement doctrine has always treated uncertainty of infringement as relevant to the question of an alleged contributory infringer's knowledge. **See Mini Maid**, 967 F.2d at 1521 (instructing district court to consider extent and nature of alleged infringement in determining whether to impute knowledge to alleged contributory infringer); Restatement (Third) of Unfair competition §26 cmt. a (993) (noting that a person's liability for contributory infringement "depends upon the nature of the business relationship between the person and the direct infringer and the knowledge attributable to the person on the basis of that relationship"). A trademark owner's demand letter is insufficient to resolve this inherent uncertainty. **Coca-Cola Co., v. Snow Crest Beverages**, 64 F.Supp. 980 (D. Mass. 1946), **aff'd**, 162 F.2d 280 (1st. Cir. 1947), a seminal contributory infringement case, addressed the contention offered here by Lockheed that an attorney's demand letter should be sufficient to impute knowledge of infringement. There, Coca-Cola asserted that Snow Crest had contributorily infringed its mark by selling "Polar Cola" to bartenders who sometimes mixed the soda into customers' "rum and Coke" drinks. **Coca-Cola**, 64 F.Supp. at 989. Coca Cola asserted that Snow Crest should have known about the infringement because Coca-Cola's counsel had told Snow Crest's president of the bartending practice. The court found that such "lawyer's argumentative talk" was insufficient to establish that a reasonable business person in Snow Crest's position should have concluded that its products were being used to infringe. **Id.** at 990. The court reasoned that if it imputed knowledge to the defendant based on Coca-Cola's blanket demand, the court would be expanding Coca-Cola's property right in its trademark, allowing Coca-Cola to secure a monopoly over the entire mixed drink trade **Id.** The same reasoning applies here. Lockheed's argument would require the Court to impute knowledge of infringement to NSI in circumstances where the use of the term "skunk works" in a domain name may or may not be infringing. Such an expansion of contributory liability would give Lockheed a right in gross to control all uses of "skunk works" in domain names.

Lockheed relies on a copyright contributory infringement case, **Religious Technology Center v. Netcom On-Line Communication Servs., Inc.**, 907 F.Supp. 1361 (N.D. Cal. 1995), for the proposition that only a low level of certainty as to infringement should be required to impute knowledge to NSI. There, the court rejected an Internet service provider's argument that its knowledge of infringement must be unequivocal in order for it to face contributory liability. **Id.** at 1374. At the same time the court noted that a "mere unsupported allegation of infringement by a copyright owner" is not enough to impute knowledge to an Internet service provider. **Id.** The court noted that where infringement is uncertain for a variety of reasons such as lack of copyright notice or a colorable fair use defense, the Internet service provider's "lack of knowledge will be found reasonable and there will be no liability for contributory infringement ... ." **Id.** Because the property right protected by trademark law is narrower than that protected by copyright law, liability for contributory infringement of a trademark is narrower than liability for contributory infringement of a copyright. **Sony Corp. v. Universal City Studios, Inc.** 464 U.S. 417, 439 n.19, 104 S.Ct. 774, 787 n. 19, (1984). Unlike trademark law, copyright law gives owners a generalized right to prohibit all copying, provided that the owner's rights are valid and the material copied is original. **Feist Publications, Inc. v. Rural Tel. Serv. Co.**, 499 U.S. 340, 360 111 S.Ct. 1282, 1296 (1991). Trademark law, on the other hand, tolerates a broad range of non-infringing uses of words that are identical or similar to trademarks.

2. Knowledge as to Specific Registrants

Lockheed's complaint alleges contributory infringement in connection with four specific registrations of SKUNK WORKS-type domain names. In addition, Lockheed has submitted evidence in opposition to summary judgment of four subsequent registrations of domain names similar to SKUNK WORKS. (Quinto Decl. Ex. E, H, L, M.) As to all of the domain name registrations, the Court finds that the alleged infringing activity did not give NSI knowledge or reason to know that its domain name registration service was being used to infringe Lockheed's service mark.

Two of the four original registrants never used their domain name in connection with a Web site or other form of Internet communication that would create a likelihood of confusion. [10] The other two registrants used their domain names, one in association with Web site, [11] and one as an e-mail address. [12] As discussed above, however, NSI is not involved with uses of domain names in connection with Internet resources such as Web sites and e-mail. Therefore, the Court cannot impute knowledge of potential infringement merely from the fact that such uses occurred. NSI, as a domain name registrar, has no affirmative duty to police the Internet in search of potentially infringing uses of domain names. **Hard Rock**, 955 F.2d at 1149 (flea market operator had no affirmative duty to take precautions against infringement by vendors); **MDT Corp. v. New York Stock Exchange, Inc.**, 858 F.Supp. 1028, 1034 (C.D. Cal. 1994). Lockheed's May 7, 1996 and June 18, 1996 demand letters do not notify NSI of any post-registration uses such as Web sites or e-mail, but merely assert that the domain names have been registered and demand their cancellation. (Quinto Decl. Exs. A & C.) Considering the uncertainty inherent in any determination that use of a domain name is infringing, the Court finds that Lockheed has failed to raise a triable issue as to NSI's knowledge of infringing uses of its services.

The parties have presented no evidence regarding use on the Internet of three of the four domain names registered since Lockheed filed its complaint. The remaining registration, that of Peter Pasho, was used in connection with a Web site. Lockheed has presented a print-out of a Web page associated with the domain name "theskunkworks.com," registered to Pasho. (Quinto Decl. Ex. N.) The Web site includes a depiction of Lockheed's SR-71 spy play and a definition of the term "skunk works" that refers to the Lockheed facility. **(Id.)** Lockheed argues that the use of the domain name "theskunkworks.com" in connection with this Web site raises the possibility of confusion over possible sponsorship by Lockheed. This argument is tenuous given the fact that the services promoted on the page are Web site design, not aerospace design. But Lockheed makes a colorable claim that where a strong mark is concerned, the use of a trademark on different products can be infringing if customers would be led to infer sponsorship. **HMH Publishing Co. v. Brincat**, 504 F.2d 713, 717 (9th Cir. 1974).

Lockheed, however, has not demonstrated that NSI was involved with or had reason to know about this Web site. NSI's management of the domain name registration process does not include a content review of Web sites and other Internet resources associated with a domain name. Although the use of the domain name "theskunkworks.com" might contribute to a likelihood of confusion as to sponsorship, NSI did not supply the domain name to Pasho. Registrants choose their own domain names. NSI, therefore, cannot be compared to a manufacturer who chooses to make generic pills that can be easily substituted for pills with protected trade dress; **Inwood**, 456 U.S. at 848-50, 102 S.Ct. at 2185-86, or a mattress manufacturer who chooses to cover box springs with fabric pattern identical to that retailed by another company. **Sealy, Inc. v. Easy Living, Inc.**, 743 F.2d 1378, 1382 (9th Cir. 1984). Nor can NSI be compared to the flea market operators who provide space, parking, food service and advertising to vendors selling infringing merchandise. If Pasho's use of the domain name "theskunkwork.com" creates a likelihood of confusion, it does so only in combination with the content of the Web page. The Web page exists on Pasho's computer or on an Internet service provider's computer. NSI does not provide computer storage, processing or communications for Web sites. NSI's role in Pasho's possible infringement is therefore not similar to the role of the flea market vendors, who provided a substantial portion of the services needed for the vendor's infringing activities, and on whose premises the infringing activities occurred. **Fonovisa**, 76 F.3d 259, 256; **Hard Rock**, 955 F.2d at 1149.

3. Conclusion as to Contributory Infringement

Lockheed bears the burden of proving that NSI induced infringement, or continued to supply a product when it knew or should have known that its customers were using the product to infringe Lockheed's mark. **See Inwood,** 456 U.S. at 853-54, 102 S.Ct. at 2188. Lockheed asserts in its Separate Statement of Genuine Issues that NSI is not entitled to summary judgment because NSI "has not adduced any evidence" regarding infringement by its registrants. (Plaintiff's Separate Statement ¶ 23.) It is not NSI's burden on summary judgment to negate the elements of Lockheed's case. The moving party on summary judgment need not produce evidence showing the absence of a genuine issue of material fact with respect to issues on which the non-moving party bears the burden of proof at trial. **Celotex Corp. v. Catrett**, 477 U.S. 317, 325, 106 S.Ct. 2540, 2554 (1986). The moving party need only point out to the

district court that there is an absence of evidence to support the non-moving party's case. **Id.**

NSI has met this burden. Lockheed's evidence would only establish liability for contributory infringement if NSI had an affirmative duty to police the Internet for infringing uses of Lockheed's service mark. No such duty exists. Lockheed's evidence does not show that NSI was involved in infringing activity or that it knew or had reason to know that its services were being used to infringe Lockheed's service mark. The Court finds that knowledge of infringement cannot be imputed to NSI because of the inherent uncertainty of trademark protection in domain names. Even after receiving Lockheed's demand letters NSI would not have reason to know that the holders of SKUNK WORKS-type domain names were infringing. Trademark law does not give Lockheed the right to interfere with all uses of the term "skunk works" by current domain name holders. Because of the inherent uncertainty of a trademark owner's right to stop others from using words corresponding to the owner's trademark in a domain name, the Court finds that an extension of contributory liability here would improperly broaden Lockheed's property rights in its service mark.

III. Conclusion

The Court finds that NSI's use of domain names is connected with their technical function to designate computers on the Internet, not with their trademark function to identify the source of goods and services. Because Lockheed cannot establish that NSI has used its service mark in connection with goods or services or with the sale, offer for sale, distribution or advertising of goods and services, the Court grants summary judgment for NSI on the direct infringement and unfair competition claims under 15 U.S.C. §§1114(1), 1125(a).

Because the Court finds that NSI's acceptance of domain name registrations is not a commercial use within the meaning of the Federal Trademark Dilution Act, 15 U.S.C. §1125(c), the Court grants summary judgment for NSI on the dilution claim.

Because NSI has demonstrated that Lockheed cannot establish that NSI knew or had reason to know that its domain name registration service was used to infringe Lockheed's mark, the Court grants summary judgment for NSI on the contributory infringement claim.

Because summary judgment on the above claims is based on Lockheed's lack of a legal right to control the domain name registration process, there is no case or controversy between these parties. Therefore, the Court grants NSI's motion for summary judgment as to Lockheed's declaratory judgment cause of action.

If the Internet were a technically ideal system for commercial exploitation, then every trademark owner would be able to have a domain name identical to its trademark. But the parts of the Internet that perform the critical addressing functions still operate on the 1960s and 1970s technologies that were adequate when the Internet's function was to facilitate academic and military research. Commerce has entered the Internet only recently. In response, the Internet's existing addressing systems will have to evolve to accommodate conflicts among holders of intellectual property rights, and conflicts between commercial and non-commercial users of the Internet. "In the long run, the most appropriate technology to access Web sites and e-mail will be directories that point to the desired Internet address. Directory technology of the necessary scale and complexity is not yet available, but when it is developed it will relieve much of the pressure on domain names." **Domain Name System, Hearing Before the Subcommittee on Basic Research of the House Science Committee**, 105th Cong., 1997 WL 14151463 (September 30, 1997) (testimony of Barbara A. Dooley, Executive Director, Commercial Internet Exchange Association). No doubt trademark owners would like to make the Internet safe for their intellectual property rights by reordering the allocation of existing domain names so that each trademark owner automatically owned the domain name corresponding to the owner's mark. Creating an exact match between Internet addresses and trademark will require overcoming the problem of concurrent uses of the same trademark in different classes of goods and geographical areas. Various solutions to this problem are being discussed, such as a graphically-based Internet directory that would allow the presentation of trademark in conjunction with distinguishing logos, new top-level domains for each class of goods, or a new top-level domain for trademarks only. The solution to the current

difficulties faced by trademark owners on the Internet lies in this sort of technical innovation, not in attempts to assert trademark rights over legitimate non-trademark uses of this important new means of communication.

DATED: November 17, 1997

DEAN D. PREGERSON

United States District Judge

FOOTNOTES

1. [Return to Text] One solution to this problem is for businesses to stake their claims on higher level domain names. For example, a business could use an Internet service providers's second-level domain and place its trademark in the third-level domain. Thus, if Acme Plumbing uses the Microsoft Network, its web site could be at America Online with the address "acme.aol.com." The drawback of this solution is that it requires customers to guess as to the second-level domain.

2. [Return to Text] Although NSI's policy does not refer explicitly to interpleader actions, NSI has attempted to deposit domain names in the registry of the court by bringing interpleader actions. None of the actions have been successful. (Graves Depo. at 104-05.) In the one reported case arising from this interpleader policy, the district court dismissed NSI's interpleader action. **Network Solutions Inc. v. Clue Computing Inc.**, 946 F.Supp 858 (D. Colo 1996). Clue Computing had sued NSI in state court to prevent cancellation of its domain name registration, "clue.com," at the behest of Hasbro, Inc., which sought to use the domain name for a Web site based on the board game "Clue." Hasbro had presented NSI with the federal registration of Hasbro's CLUE trademark, and demanded that NSI cancel Clue Computing's domain name registration. NSI attempted to extricate itself from between the two claimants by filing a interpleader action. However, the district court found that NSI was not a disinterested stakeholder because Clue Computing had accused it of breaching the domain name registration contract. 946. F.Supp. at 861.

3. [Return to Text] The Court takes judicial notice of a draft document prepared by the staff in the Office of the Assistant Commissioner for Trademarks of the United States Patent and Trademark Office entitled "Observations Concerning the Examination of Applications for Registration of Domain Names in the Trademark Office." This document directs trademark examiners to determine whether a domain name submitted for trademark registration functions only as a locator of a business on the Internet, in which case registration should be refused because the domain name is not serving a trademark function. While the Court's conclusion does not depend on this document or any Patent and Trademark Office policy that it might reflect, the Court notes that trademark examiner practice is consistent wit the view that the registration or a domain name with NSI for use on the Internet, without more, is not a commercial use of the name as a trademark under the Lanham Act. **See also,** 2 Gilson, **supra**, § 5.11 [5], at 5-243-44 (noting Patent and Trademark Office practice regarding use-based registration of domain names as trademarks).

4. [Return to Text] It is important to note that impending access to a domain name is not the same thing as impending access to the Internet. Even if the trademark owner cannot establish a "vanity" domain name, the owner remains free to promote the trademark on the Internet by using the trademark in the content of a web site. A web site's content is not connected to or restricted by the domain name under which it is accessed. **See** David J. Loundy, **A Primer on Trademark Law and Internet Addresses,** 15 J. Marshall J. Computer & Info. L. 465, 480 n. 86 (1997). In addition, the trademark owner may use the trademarked words as a third-level domain name, or as a second-level domain name in combination with letters that distinguish it from previously registered second-level domains. A domain name dispute between Acme Plumbing and Acme Pizza, for example, can be resolved by adding more information to the second-level domain names, as in "acmeplumbing.com" and "acmepizza.com."

5. [Return to Text] NSI objects to the IPO as inadmissible hearsay. The IPO is admissible as an admission of a party opponent. Fed.R.Evid 801 (d)(2).

6. [Return to Text] Lockheed asserts that NSI's domain name dispute policy requires registrants to use their domain names. (Quinto Decl. in Opp'n to Ex Parte Application for Civil Contempt ¶ 8.) Lockheed points to the section of the policy that requires registrants "to have operational name service from at least two operational domain name servers ... ." **(Id.,** Ex. E.) This language is quoted from a section of the policy under the heading "Connectivity." This section does not require the registrant to connect the domain name with any content on the Internet, such as a web site. It merely requires the registrant to secure the use of two domain name servers to list the domain name in connection with an IP number. Requiring registrants to link their domain names with IP numbers is not the same thing as requiring registrants to use their domain names on the Internet.

7. [Return to Text] The Court notes, however, that the tort law analogy used in **Fonovisa** and **Hard Rock** probably would not apply to Internet service providers and better than it applies to NSI. Even though Internet service providers directly provide the storage and communications facilities for Internet communication, they cannot be held liable merely for failing to monitor the information posted on their computers for tortious content. **See Zeran v. America Online, Inc.,** __ F.3d __, 1997 WL 701309, at *3 (4th Cir. Nov. 12, 1997) (noting that Congress created a tort immunity for Internet service providers in the Communications Decency Act of 1996, 47 U.S.C. § 230, because "[i]t would be impossible for service providers to screen each of their millions of postings for possible problems"); **but see** 47 U.S.C. § 230(d)(2) (providing that the tort immunity does not limit or expand any law pertaining to intellectual property).

8. [Return to Text] The uncertainty of Lockheed's rights over potentially generic uses of words similar to its mark is made greater in this case by the breadth of the preemptive rights asserted by Lockheed. NSI propounded an interrogatory asking Lockheed to identify all alphaneumeric strings whose inclusion in a domain name would infringe Lockheed's service mark. Lockheed objected to the interrogatory as unduly burdensome, and answered with 24 phrases that would infringe, including the word "skunk" (Jones Decl. Ex. 1.)

9. [Return to Text] Internet users may also have a free speech interest in non-infringing uses of domain names that are similar or identical to trademarks. **See American Civil Liberties Union of Georgia v. Miller,** __ F.Supp __, 1997 WL 552487, at *4 (N.D. GA. June 23, 1997) (invalidating as overbroad statute that criminalized certain uses of trademarks on the internet by persons other than trademark owner because statute would have prohibited "use of trade names or logos in non-commercial educational speech, news, and commentary -- a prohibition with well-recognized First Amendment problems").

10. [Return to Text] Seng-Poh Lee's "skunkworks.com" name was used to established an e-mail forwarder. Mr. Lee never received or sent e-mail using the domain name. (Jones Decl. Ex. 3.) After receiving a cease-and-desist letter from Lockheed, Mr. Lee canceled his domain name registration. The domain name became generally available and was registered to a new user, Grant Smith, in 1996.

Ken Hoang's "skunkworks.net" was not used in association with a web site or any other Internet form of communication. (Jones Decl. Ex. 6.)

11. [Return to Text] Roger Barski's "skunkworks.com" domain name was associated with a web site offering Mr. Barski's services as a web site designer. (Jones Decl. Ex. 5.) After receiving Lockheed's cease-and-desist letter. Mr. Barski canceled the Internet service provider account that had supplied domain name service for "skunkworks.com." Without domain name service, the domain name is effectively removed from the Internet, because users who attempt to access Internet resources associated with the domain name receive only an error message. **(Id.).**

12. [Return to Text] Kathy Huber's "skunkwrks.com" was not associated with a Web site, but was associated with an e-mail address for Ms. Huber's former company, Skunkworks Marketing Labs. (Jones Decl. Ex. 4).

© 1997 The Bureau of National Affairs Inc., All Rights Reserved

TITLE II--ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION

SEC. 201. SHORT TITLE.

This title may be cited as the 'Online Copyright Infringement Liability Limitation Act'.

SEC. 202. LIMITATIONS ON LIABILITY FOR COPYRIGHT INFRINGEMENT.

(a) IN GENERAL- Chapter 5 of title 17, United States Code, is amended by adding after section 511 the following new section:

'Sec. 512. Limitations on liability relating to material online

'(a) TRANSITORY DIGITAL NETWORK COMMUNICATIONS- A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if--

'(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

'(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

'(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

'(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

'(5) the material is transmitted through the system or network without modification of its content.

'(b) SYSTEM CACHING-

'(1) LIMITATION ON LIABILITY- A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which--

'(A) the material is made available online by a person other than the service provider;

'(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and

'(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the

material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A),

if the conditions set forth in paragraph (2) are met.

(2) CONDITIONS- The conditions referred to in paragraph (1) are that--

'(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A);

'(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies;

'(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology--

'(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;

'(ii) is consistent with generally accepted industry standard communications protocols; and

'(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person;

'(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and

'(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if--

'(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and

'(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.

'(c) INFORMATION RESIDING ON SYSTEMS OR NETWORKS AT DIRECTION OF USERS-

'(1) IN GENERAL- A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider--

'(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

'(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

'(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

'(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

'(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

'(2) DESIGNATED AGENT- The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:

'(A) the name, address, phone number, and electronic mail address of the agent.

'(B) other contact information which the Register of Copyrights may deem appropriate.

The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

'(3) ELEMENTS OF NOTIFICATION-

'(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

'(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

'(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

'(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

'(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

'(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

'(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

'(B)(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

'(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

'(d) INFORMATION LOCATION TOOLS- A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider--

'(1)(A) does not have actual knowledge that the material or activity is infringing;

'(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

'(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

'(2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

'(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.

'(e) LIMITATION ON LIABILITY OF NONPROFIT EDUCATIONAL INSTITUTIONS- (1) When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research function, for the purposes of subsections (a) and (b) such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) such faculty member's or graduate student's knowledge or awareness of his or her infringing activities shall not be attributed to the institution, if--

'(A) such faculty member's or graduate student's infringing activities do not involve the provision of online access to instructional materials that are or were required or recommended, within the preceding 3-year period, for a course taught at the institution by such faculty member or graduate student;

'(B) the institution has not, within the preceding 3-year period, received more than two notifications described in subsection (c)(3) of claimed infringement by such faculty member or graduate student, and such notifications of claimed infringement were not actionable under subsection (f); and

'(C) the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright.

'(2) INJUNCTIONS- For the purposes of this subsection, the limitations on injunctive relief contained in subsections (j)(2) and (j)(3), but not those in (j)(1), shall apply.

'(f) MISREPRESENTATIONS- Any person who knowingly materially misrepresents under this section--

'(1) that material or activity is infringing, or

'(2) that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

'(g) REPLACEMENT OF REMOVED OR DISABLED MATERIAL AND LIMITATION ON OTHER LIABILITY-

'(1) NO LIABILITY FOR TAKING DOWN GENERALLY- Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.

'(2) EXCEPTION- Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider--

'(A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material;

'(B) upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and

'(C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.

'(3) CONTENTS OF COUNTER NOTIFICATION- To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:

'(A) A physical or electronic signature of the subscriber.

'(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.

'(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

'(D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.

'(4) LIMITATION ON OTHER LIABILITY- A service provider's compliance with paragraph (2) shall not subject the service provider to liability for copyright infringement with respect to the material identified in the notice provided under subsection (c)(1)(C).

'(h) SUBPOENA TO IDENTIFY INFRINGER-

'(1) REQUEST- A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.

'(2) CONTENTS OF REQUEST- The request may be made by filing with the clerk--

'(A) a copy of a notification described in subsection (c)(3)(A);

'(B) a proposed subpoena; and

'(C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

'(3) CONTENTS OF SUBPOENA- The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.

'(4) BASIS FOR GRANTING SUBPOENA- If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.

'(5) ACTIONS OF SERVICE PROVIDER RECEIVING SUBPOENA- Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.

'(6) RULES APPLICABLE TO SUBPOENA- Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

'(i) CONDITIONS FOR ELIGIBILITY-

'(1) ACCOMMODATION OF TECHNOLOGY- The limitations on liability established by this section shall apply to a service provider only if the service provider--

'(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and

'(B) accommodates and does not interfere with standard technical measures.

'(2) DEFINITION- As used in this subsection, the term 'standard technical measures' means technical measures that are used by copyright owners to identify or protect copyrighted works and--

'(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;

'(B) are available to any person on reasonable and nondiscriminatory terms; and

'(C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.

'(j) INJUNCTIONS- The following rules shall apply in the case of any application for an injunction under section 502

against a service provider that is not subject to monetary remedies under this section:

'(1) SCOPE OF RELIEF- (A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:

'(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.

'(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

'(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.

'(B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following forms:

'(i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

'(ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.

'(2) CONSIDERATIONS- The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider--

'(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;

'(B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;

'(C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and

'(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

'(3) NOTICE AND EX PARTE ORDERS- Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network.

'(k) DEFINITIONS-

'(1) SERVICE PROVIDER- (A) As used in subsection (a), the term 'service provider' means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.

'(B) As used in this section, other than subsection (a), the term 'service provider' means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

'(2) MONETARY RELIEF- As used in this section, the term 'monetary relief' means damages, costs, attorneys' fees, and any other form of monetary payment.

'(l) OTHER DEFENSES NOT AFFECTED- The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.

'(m) PROTECTION OF PRIVACY- Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on--

'(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or

'(2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.

'(n) CONSTRUCTION- Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that

subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.'.

(b) CONFORMING AMENDMENT- The table of sections for chapter 5 of title 17, United States Code, is amended by adding at the end the following:

'512. Limitations on liability relating to material online.'.

SEC. 203. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect on the date of the enactment of this Act.

Cooley Godward LLP

Article Reprints

The Intellectual Property Renaissance In Cyberspace: Why Copyright Law Could Be Unimportant On The Internet

August 14, 1997
by Eric Goldman

TABLE OF CONTENTS

I. INTRODUCTION

Influential futurist Ithiel de Sola Pool wrote:

> For copyright, the implications [of electronic publishing] are fundamental. Established notions about copyright become obsolete, rooted as they are in the technology of print. The recognition of a copyright and the practice of paying royalties emerged with the printing press. With the arrival of electronic reproduction, these practices become unworkable. Electronic publishing is analogous not so much to the print shop of the eighteenth century as to word-of-mouth communication, to which copyright was never applied.(1)

The emergence of electronic networks has undeniably placed significant pressure on our existing intellectual

property system. As with each new technological advance, copyright law must adjust to fit the new circumstances presented by the Internet. Until law and technology reach an equilibrium, many predict that intellectual property creators will be reluctant to create works for the Internet environment since creators will be unable to protect their copyright interests.(2) Others have argued that only minor adjustments are necessary to fit copyright law to electronic networks such as the Internet.(3) Still others--a distinct minority--believe that copyright law has become less important in the age of electronic networks, and that production of intellectual property will continue unabated even without powerful copyright rights.(4)

Unlike Professor Pool, we have the benefit of a few years of empirical evidence to draw upon in analyzing the effects of electronic networks on intellectual property. This article analyzes some of the lessons we have learned in the commercial Internet's toddler years to glean some insights into the implications for copyright law and Internet-based commerce. After analyzing recent economic, business, sociological and technological developments, this article concludes that, while copyright law has a role to play on the Internet, other developments overshadow copyright law as a tool for conforming behavior such that copyright law may be unimportant to the Internet. The public policy implications are clear: the business models, sociology and technology of the Internet are evolving so rapidly that efforts to conform copyright law to this environment would be detrimental.

Part II summarizes a few basic points of U.S. copyright law. Part III describes specific threats that the Internet poses to the enforcement of rights under copyright law. Part IV analyzes the economics of electronic networks to identify why intellectual property might be created even in a putatively anarchistic, piracy-infested environment such as the Internet. Part V discusses sociological attitudes towards intellectual property on the Internet, identifying why it will be difficult to conform behavior on the Internet to the strict letter of existing copyright laws. Part VI discusses technologies that copyright holders can use in the battle over works subject to copyright. Finally, part VII concludes with thoughts about how we can live in a world where copyright laws are not the primary influence on our behavior towards intellectual property.

II. UNITED STATES COPYRIGHT LAW BASICS(5)

Many excellent summaries of U.S. copyright law exist,(6) and this section will not attempt to duplicate those efforts. However, mapping out the basic contours of the existing U.S. copyright law scheme is helpful in understanding the import of the conclusions of this article.

The Constitution authorizes Congress to establish a legislative scheme "to promote Science and the useful Arts, by securing for limited Times to Authors . . . the exclusive right to their . . . writings...."(7) In response, Congress enacted the Copyright Act of 1909, which it later replaced with the Copyright Act of 1976 (the "Copyright Act").(8)

The Copyright Act governs original works of authorship that are fixed in a tangible medium of expression. While the standard for originality is low, facts and ideas may not be copyrighted.(9) For copyrightable works, the owner has the following exclusive rights:

> (1) to reproduce the copyrighted work in copies or phonorecords;
>
> (2) to prepare derivative works based upon the copyrighted work;
>
> (3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
>
> (4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly;
>
> (5) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and
>
> (6) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.(10)

These exclusive rights are subject to numerous restrictions. First, in the case of works created after January 1, 1978, these rights cease 50 years after the death of the author, or, in the case of works made for hire, the earlier of 75 years from the date of first publication or 100 years from the date of creation.(11)

Second, these exclusive rights are subject to the doctrine of fair use, which may permit the infringement of an exclusive right of a copyright owner if its conditions are met. The Copyright Act enumerates four factors that are to be considered to determine whether or not a use is fair:

(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

(2) the nature of the copyrighted work;

(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

(4) the effect of the use upon the potential market for or value of the copyrighted work.(12)

In evaluating a claim of fair use, the court is to consider all four factors. However, taking 100 percent of a copyrighted work ordinarily militates against a finding of fair use,(13) and the fourth factor is generally considered the most important.(14)

There are numerous other statutory exceptions and limitations to copyright owners' rights, generally set out in Sections 108 to 120 of the Copyright Act.

Other intellectual property rights in U.S. law often also apply to works for which copyright protection is sought, including trade secret rights, trademark rights, patent rights, rights of publicity, and rights of privacy. While these other forms of intellectual property are not addressed in this paper, collectively they form an important additional basket of rights available to creators of intellectual property.

III. THREATS TO ENFORCING COPYRIGHT RIGHTS ON THE INTERNET

This section describes some of the unique ways that the Internet poses a threat to copyright owners' ability to enforce their copyrights.

A. No Loss of Quality In Reproduction

Unlike copies of intellectual property made using analog copiers (such as photocopy machines, video and music tape recorders, facsimile machines and others), digital copies of intellectual property produce perfect copies without any loss of quality. The first generation and the 1000th generation copy of digital material are indistinguishable. Since each copy is a perfect copy, no quality-related limits inhibit pirates from making as many copies as they please, and recipients of these copies have no incentive to return to authorized sources to get another copy equal in quality to the original version.

B. No Meaningful Marginal Costs of Reproduction or Distribution

Unlike the business of selling and distributing physical copies of books, magazines, music cassettes or CDs, video cassettes or software, the costs of making one extra copy of intellectual property on-line are insignificant, as are the distribution costs associated with moving that copy to the end user over the Internet. Assuming no per-byte or other volume costs are imposed on the site owner (which is the current state of the market), infringement can occur at virtually no marginal cost.

C. Ability to Act Anonymously

Using anonymous remailers and other existing technologies, pirates are able to act anonymously on-line, leaving no traceable trail of activity. Anonymity poses a significant threat on the Internet, because it theoretically allows pirates to cause harm without bearing any risk of loss, thus undermining the general presumption that those causing harm can be forced to internalize the costs of their actions. As a result, more infringement is likely to occur than if costs were properly internalized.

However, anonymous activity is not a copyright-specific problem; it applies to all crimes and torts that can be committed on-line. Therefore, it may be more appropriate to address the harm caused by anonymity generally, rather than drafting a specific resolution applicable only to losses suffered by copyright owners. Furthermore, there is a built-in limitation to the scope and size of anonymous actions, particularly if any element of the activity is commercial; at a certain point the activity should become large enough to leave at least shreds of evidence, both in physical space and cyberspace, sufficient to allow attribution.(15)

D. Uneducated Users

Many users do not understand the existing copyright legal framework.(16) While the lack of user education applies in both physical space and cyberspace, the Internet permits these users to widely disseminate works with relative ease. Often times, this publication can inadvertently cause harm, such as the forwarding of works subject to copyright to third parties. The result may be a number of relatively small infringements that, in the aggregate, can lead to significant losses for copyright holders.

E. Conclusion

The foregoing threats indicate that copyright holders face substantial risks on-line. Nevertheless, we already have ample evidence that intellectual property is still being created for distribution on the Internet. Indeed, a staggering—almost unmanageable--quantity of intellectual property continues to be produced and made available on-line despite these threats.(17) Therefore, despite the assertions of those who believe that the threats posed on-line to copyrighted works would result in disincentives to create and distribute works, it appears other forces are at work on the Internet.

IV. ECONOMICS AND THE INTERNET

This section applies economic theory and surveys existing business models to suggest why, without increased copyright protection, intellectual property is still likely to be produced even if it is given away on the Internet.

A. Price-Setting Behavior in a Nearly Efficient Marketplace When Marginal Costs Are Meaningfully Zero

The Internet is not a perfectly efficient market, but it does represent a close approximation. Among the requirements for an efficient market are perfect information and zero transaction costs. First, while the Internet does not offer perfect information, some industries provide enough information on the Internet to give buyers an opportunity to compare prices based on nearly perfect information.(18) On the Internet, it is likely that many additional industries will experience this phenomenon. Second, while transaction costs are not zero, the Internet has significantly reduced transaction costs. In particular, buyers may experience no marginal transaction costs attributable to using the Internet for finding purchasing opportunities or consummating a transaction.(19)

In an efficient marketplace, a firm's profit-maximizing price is the price where marginal revenue from each sale of the product equals the marginal costs of the product.(20) If marginal costs are zero, what is the profit maximizing price?

1. Marginal Costs on the Internet

For many intellectual property creators, the marginal cost of each additional "sale" of the intellectual property is likely to be effectively zero. While many costs are associated with producing intellectual property, including the time of the creator and the Internet infrastructure (such as the hardware, software and Internet connection), these costs become fixed costs once the intellectual property is produced.(21) At that point, if the intellectual property is uploaded to the Internet, the remaining costs are trivial--further reproduction or distribution on the Internet imposes no meaningful marginal costs.

2. Optimal Pricing

Economic theory predicts that if the marginal costs to "selling" intellectual property is zero, then some producers will accept zero marginal revenues. In other words, the profit-maximizing price for theses producers will be zero. Since this is a seemingly anomalous result, how can this be explained? There are at least four different possible explanations:

(i) A zero-revenue pricing strategy may persist only in the short run; but, ultimately, because no profits are being made, all producers will exit this business. This is fundamentally the assertion of those who believe that intellectual property owners must be paid directly for their creative efforts, or else they will not produce.(22)

(ii) The only sustainable pricing strategy may be a scheme involving price discrimination, where prices are set in accordance with users' willingness to pay. In this situation, intellectual property will be offered at varying prices, including possibly free, depending on the user.(23)

(iii) Traditional economic theory may break down on the Internet so that intellectual property will not be offered for free despite the absence of marginal variable costs. If this were true, the profit-maximizing price may not be where marginal revenue equals marginal cost. This would be a rather profound result, implicating large chunks of existing economic theory.

(iv) Finally, the profit-maximizing price on the Internet may be where marginal revenue equals marginal cost because intellectual property will be cross-subsidized by other products in a manner sufficient to cover the fixed costs associated with intellectual property creation and distribution. If this is true, a market price of zero for intellectual property can still create long-term economic profits attributable to intellectual property creation.

Of the four possible explanations, as explained in the remainder of this part IV, the author believes that the

last proposition best explains why the production and distribution of intellectual property will continue even in the absence of marginal revenues directly attributable to users of the intellectual property.

The remainder of this part IV will discuss why the last theory is at least supportable when it comes to many categories of intellectual property on the Internet.

B. Cross-subsidization of Intellectual Property Creation

There is nothing new about the proposition that vendors may give away X to sell Y. In the classic formulation of its strategy, Gillette is credited with conceiving the business model of giving away razors to sell its blades.(24) However, the deployment of this strategy is inherently limited because a razor is a tangible "thing" that will always have marginal costs to produce. On the Internet, where the marginal costs of reproduction and distribution of intellectual property are effectively zero, cross-subsidization becomes viable for a significantly greater number of products.

An intellectual property owner can use a myriad of alternative business models to extract value from the free distribution of intellectual property. If successful, these business models will permit the cross-subsidization of intellectual property creation. Internet entrepreneurs will be induced to create intellectual property if they are able to use it to make a profit from alternative revenue sources.(25)

The remainder of part IV.B provides a survey of Internet-based cross-subsidization models that may support the production of intellectual property designed to be given away freely.

1. Advertising

Advertising is one of the highest-profile business models on the Internet. Under the advertising model, a company gives away intellectual property to attract visitors to its site and then sells advertising space on its site to others. A broad range of companies are launching advertising-based attempts to freely give away intellectual property and substantive services, including email accounts,(26) interactive news agents,(27) editorial periodicals(28) and search engines and indexes.(29)

However, the slow increase in Internet advertising dollars suggests that, in the short run, advertising revenue may be insufficient to support the level of free distribution of intellectual property that exists today.(30) Because the supply of advertisement placement opportunities exceeds the demand of advertisers, advertisers are becoming more demanding.(31) Moreover, Internet users have grown weary of the often annoying banner advertisements. Nevertheless, the results obtainable from on-line advertising can be so compelling that certain advertisers have strong incentives to choose Internet advertising over other media.(32)

Furthermore, other media industries indicate that multi-billion dollar industries can be built primarily on advertising. For example, the multi-billion dollar broadcast TV industry effectively gives away its intellectual property to viewers, supporting itself almost exclusively on advertising. The television broadcasting model is consistent with the contention that Internet users will not be required to pay for intellectual property, and that the production of intellectual property can be entirely supported by advertising.

In reality, many intellectual property owners will combine the advertising model with other forms of ancillary revenues.(33) Nevertheless, advertising remains a critically important component of Internet cross-subsidization business models.

2. Sponsorships

A variant on the advertising model, sponsorship is the "co-branding" of intellectual property with the sponsor's trademarks. In the old days of television, sponsorship was common; companies would purchase all of the advertising for a show and be acknowledged as the sponsor.(34) On-line, sponsorship can take many forms, but the fundamental premise is that the sponsor will be more integrated with the content than just sticking its banner ad at the top of the page. For example, Riddler <http://www.riddler.com/home/html> promotes a contest which gives rewards to participants who can answer riddles that require the participants to visit sponsors' sites.(35)

Sponsorship is emerging as a strong alternative to banner advertising, at least partly due to advertisers' dissatisfaction with the results from banner advertising.(36) However, sponsored content also raises difficult issues about editorial integrity as the line between advertisement and editorial information becomes blurred.

3. "Try Before You Buy"

In the "try before you buy" model, companies provide consumers with a free copy of a work which is limited in some way (such as duration or functionality) in the hopes that the consumers will purchase a full copy. For

example, a vendor may give away software in the hopes that recipients will return to purchase a copy. Moreover, in many instances consumers may unilaterally pirate works and then later decide to purchase legitimate copies, even though the vendor never intended to provide "try before you buy" copies.(37) On the Internet, the "try before you buy" model has become extremely popular, in part because no meaningful marginal costs are associated with manufacturing or distributing trial copies. Thus, software,(38) content(39) and subscription services(40) are routinely given away on a "try before you buy" basis.

4. Sales of Upgrades

Under the sale of upgrades model, consumers are freely given intellectual property with the expectation that some of them will purchase a superior version. In some ways a variant of the "try before you buy" model, this model capitalizes on the fact that version 1.0 of a product can be the best device to sell version 2.0. For example, sales of upgrades are ubiquitous in the modem software business, where companies bundle their "lite" version of software with the modem for free in the hope that consumers will upgrade to the "professional" version. However, the model is not limited to software; an author might give away a short story as a way to build demand for a "further adventures" sequel story or the movie.(41)

5. Sale of Complementary Technology

The truest application of Gillette's maxim, the Internet version might be "give away the client software to sell the server software." For example, the Internet's "browser software wars" have focused heavily on the free distribution of client software. With a large installed base of client software, the server software--which is sold and provides added functionality for people using the client software--becomes more attractive. More generally, software companies who also have hardware businesses may give away software to encourage the use of complementary proprietary hardware.(42)

6. Sales of Physical Goods

Companies may use the free distribution of intellectual property to foster the sale of physical goods in many ways. For example, Digital initially intended to popularize its Alta Vista search engine in order to showcase the speed of its Alpha servers.(43) Digital thus intended to give away a search tool as a way to enhance sales of its physical goods. Similarly, in the area of character merchandising, many companies may seek to build character awareness on-line through free distribution of character-related content; the increased character awareness may translate into increased demand for character-branded merchandise.(44) Finally, electronic distribution of intellectual property could be used to create demand for physical copies of intellectual property that have been bolstered with additional content or experience-enhancing elements.(45)

7. Sales of Services

Companies may stimulate demand for services by distributing free intellectual property on-line. For example, consultants may find it relatively easy to attract potential customers by distributing free content that demonstrates expertise. Alternatively, software companies can give away software as a way to sell systems integration or customized application development.

A notable example of the use of cross-subsidization to sell services is the free distribution of software as an avenue to sell technical support. For example, Microsoft gives away its Internet Explorer browser without a licensing fee, but users must purchase technical support. The sale of technical support unbundled from the underlying software has become increasingly popular.

8. Personal Information Collection and Data Mining

Internet sites can easily collect a fair amount of information about their users, much of it without the user's consent. For example, Internet sites can learn the user's IP address and most recently visited site. Furthermore, by placing a unique identifier into the user's "cookie"(46) (or, with less precision, by analyzing the server logs), the Internet site can trace the user's activity through the site and glean insights into what the user looks at and for how long. In addition, many sites may request or require users to fill out registration forms which call for the disclosure of extensive personal information.

Companies can then exploit this information for commercial gain in a number of ways, such as selling email mailing lists to other companies or selling advertising space to companies that want to provide users with customized product offerings or page views based on their perceived preferences.(47) Although the commercial use of this personal information can create some significant privacy issues,(48) such use is generally not subject to legal restrictions in the United States.

9. Communities

The Internet is particularly useful for facilitating community formation. In physical space, community

formation may be inhibited by geography, the cost of communication, or the asynchronous methods of communication. On the Internet, however, groups can form quickly and cheaply since these barriers are absent. Moreover, the absence of these barriers may facilitate the formation of communities devoted to extremely narrow topics, which otherwise would not form.

The formation of Internet communities offers one of the most promising Internet business opportunities. If an Internet site can successfully attract like-minded people to interact with each other on the site, it will have a number of ways to extract value from these relationships.(49) In addition to the obvious methods, such as selling the demographics to advertisers and selling the mailing list to merchants interested in reaching the target audience, the Internet site can extract value by enhancing the community members' ability to communicate with each other. The site could accomplish this by providing proprietary tools to facilitate onsite communication and tools and methods to facilitate and enrich physical-space meetings between members.

For example, WebGenesis <http://www.theglobe.com> provides chat rooms oriented primarily towards young adults. While the general public can access the chat rooms for free, subscribers receive "bonus" onsite privileges, including an onsite home page to which all their onsite chat postings are hypertext linked automatically, access to private chat rooms available only to other subscribers (who presumably are also dedicated chatters), and the ability to use tools such as Java that enhance the chatting experience. In other words, by providing the chat rooms for free, WebGenesis is able to identify those members of the communities who desire a greater relationship to the community and target these people for the sale of advanced onsite communications products.

Companies could also derive revenue opportunities from Internet communities by organizing conferences and other events of interest to the community. A site that forms a community dedicated to river rafting, for example, could sell river rafting trips to its members, an endeavor that would have the added value of creating an opportunity to meet other members of the community in physical space.

10. Reinforcement of Physical-Space Messages

Internet sites can be used to reinforce marketing and sales efforts being made elsewhere. Such reinforcement can occur in the form of customer support and outreach, such as Federal Express' <http://www.fedex.com/>, use of its website to provide data tracking services to its customers, or a software company's use of the Internet to distribute bug fixes, FAQs, usage tips and other forms of customer assistance.

Alternatively, some companies use Internet sites to increase customer loyalty or provide branding opportunities.(50) For example, the websites prepared by Zima <http://www.zima.com/> and Miller Genuine Draft <http://www.mgdtaproom.com/> contain offerings designed to allow their consumers to feel like the part of a community and to encourage brand loyalty. The Internet market has been described as a "relationship" market;(51) free intellectual property can be the way to initiate, build or reinforce the relationship.

C. Importance of Attribution

As the prior section has indicated, companies can try a myriad of methods of creating value by giving away intellectual property. However, for cross-subsidization to work, buyers impressed with product X (freely given away) must be led to product Y (for sale). In most cases, this will mean that product X must give proper attribution to the seller of product Y so that buyers can make the connection. U.S. copyright law affords no "right of attribution" to owners of intellectual property distributed on the Internet.(52) While some trademark, unfair competition, or right of publicity theories may limit the ability of users of intellectual property to falsely represent the origin of the intellectual property, there is no copyright obligation of attribution.(53)

In some cases, attribution may be the only right that matters on the Internet. In fact, an intellectual property owner seeking cross-subsidization may encourage people to "infringe" the intellectual property through wide distribution, so long as attribution is given.(54) Thus, existing copyright law lacks an important right, the absence of which could hinder the deployment of key business models on the Internet.

The NII White Paper recognized that attribution could be important and therefore recommended that copyright law be amended to "prohibit the provision, distribution or importation for distribution of copyright management information known to be false and the unauthorized removal or alteration of copyright management information."(55) The White Paper defines copyright management information as the name of the copyright owner and the terms and conditions for use of the work.(56)

While not adopted into law in the United States, a virtually identical proposal was adopted at the proceedings of the World Intellectual Property Organization ("WIPO").(57) Time will tell if the treaty will be adopted without changes in the United States.

The White Paper proposal and the WIPO treaty represent an important step toward the recognition of the

right of attribution in the United States. However, the proposed law could have profound effects on some current Internet practices.(58) First, website operators commonly incorporate content maintained on remote servers into the pages delivered to users through a direct hypertext link to the remote content.(59) Intellectual property owners whose files are linked this way may object (1) because these direct-linked users do not actually visit their site, and (2) because the file may be displayed so as to suggest that the site providing the link is the source of the file. Does this form of direct linking run afoul of the White Paper's proposal? Should it? Would it matter if the linked-to site provided a notice denying access to others who attempted to link to the site? (60)

Second, robots and agents can, for example, survey multiple search engines and display the search results to the end user in summary form, without displaying any advertising contained on the search engine's site (or, for that matter, giving any attribution to the search engine).(61) As a result, the search engine sites must bear the costs of providing the service without getting the anticipated benefits from the consumers of the information. Does this type of robot behavior run afoul of White Paper's proposal? Should it? Would it matter if the search engine's site contained a notice that notified others that robots and agents were not welcome?

D. Conclusion

The large number of alternative business models presented above is necessarily incomplete; entrepreneurs have proven highly capable of developing new ways of extracting value from the Internet. However, the mere existence of so many alternatives reinforces the fundamental message: intellectual property creators can cross-subsidize the production of their works in many ways.

The impact of this concept is powerful: if even one person is able to produce and freely distribute a type of intellectual property through cross-subsidization, why would consumers continue to pay for an equivalent work? While each copyrightable creation is theoretically unique, many types of intellectual property have substitutes which consumers would readily choose if they were available for free.(62) In other words, if the Internet is a relatively efficient market and intellectual property is somewhat fungible, then the free availability of a type of work should establish the market price for that type of intellectual property at zero.(63)

The implications of this proposition are truly profound. It suggests that intellectual property owners who expect to be paid directly by end users will face extreme competitive pressures. A single entrepreneur able to cross-subsidize the production of substitute intellectual property should theoretically drive the market price to zero and eliminate all prospects that end users will directly pay for the intellectual property. Given the plethora of methods an entrepreneur could use to achieve this result, zero pricing may be inevitable for many classes of intellectual property.

However, some categories of intellectual property almost certainly will not be given away for free.(64) For those categories that will support user payments, entrepreneurs can deploy various technologies to protect their intellectual property and increase the likelihood of payment. These technologies are discussed in part VI.

V. SOCIOLOGY OF THE INTERNET

While business and technological factors significantly impact the market for intellectual property, some noteworthy features about users' attitudes towards intellectual property also warrant attention. This section describes certain sociological aspects of the Internet culture and how they may influence users' willingness to pay.

A. Attitudes Towards Intellectual Property

Attitudes towards intellectual property can be placed on a spectrum ranging from "intellectual property should not be protected" to "intellectual property should be highly protected." Though not discrete nodes, five distinguishable segments of this spectrum can be identified:(65)

1. Information Wants to be Free

Adherents to this perspective believe that any intellectual property should be in the public domain and available for all to use. While finding dogmatic adherents to this perspective may be difficult, finding people who believe that anything they find on the Internet is "fair game" for free use is relatively easy.

2. Right of Attribution

Adherents to this perspective believe that intellectual property can be freely "infringed" so long as the source is attributed. Again, though it may difficult to find people who strictly adhere to this perspective, it is very easy to find people--even among creators of intellectual property--who subscribe to this perspective at least some of the time. Interestingly, U.S. copyright law rarely requires attribution (see part IV.C, *supra*), although

netiquette usually encourages it.

3. Limited Use of Works Subject to Copyright

Adherents to this perspective believe that intellectual property creators should have protectable rights in their creations, but they do not believe that these rights are absolute. Often, adherents want to strike a balance between protecting creators' interests and permitting "infringement" of the intellectual property in a manner consistent with their lifestyle or business. This position arguably represents the framework for existing U.S. copyright law, which gives significant protection to copyright holders but provides the fair use defense and statutory exemptions.

4. Moral Rights

"Moral rights" are the rights of the author to be attributed as the author of the work and to object to a particular use of the work.(66) As between the author and any potential user (including assignees or licensees), this perspective strongly favors the author; often the author cannot assign his or her rights, and in some jurisdictions the author cannot waive the enforcement of his or her moral rights.(67) Generally, moral rights reflect a belief that the author's creations are an extension of the author, and therefore the author can control how the public views author through his or her creations. U.S. copyright law does not explicitly recognize moral rights except in a very limited set of circumstances.(68)

5. Strong Intellectual Property Rights

Adherents to this perspective believe that the author should have significant power to control the use of his or her intellectual property. Adherents would extend the author's power beyond moral rights and permit the author to control all uses of his or her work.

From a policy perspective, it is useful to think about how our copyright laws can conform the behavior of people who subscribe to the perspectives outlined above. Importantly, people who subscribe to the "information wants to be free" theory may very well abuse copyright restrictions regardless of the strength of intellectual property laws, in which case strengthening copyright laws to conform their behavior serves little purpose.(69)

To the extent that the Internet culture has increased the number of people unsupportive of strong intellectual property rights, new copyright laws designed to increase creators' rights are unlikely to produce the desired results.

B. Internet Culture and Micro-Infringements

Historically, the Internet has been populated by academics and technologists, many of whom would properly be categorized in the "Information Wants to be Free" segment (or perhaps the "Right of Attribution" segment) of the intellectual property attitude spectrum.(70) While waves of newcomers to the Internet have diluted this culture, many of these newcomers bring complementary attitudes towards intellectual property.

Take, for example, people under the age of thirty. During most or all of their life, they have had easy access--often in their home--to a number of devices they could use to infringe copyrights: audio cassette recorders (and cheap blank tapes); video cassette recorders (and again cheap blank tapes); high quality, low cost photocopy machines; fax machines; and perhaps the most powerful copying device of all, the personal computer (and cheap blank disks and hard drives). As a result, the under-thirty generation has grown up being able to freely expropriate intellectual property easily and at little cost.(71) As college students, how many of them bought most (or even some) of the software on their computer, rather than "borrowing" it from their folks or from a friend down the hall? How many of them put together a compilation tape of their favorite songs? How many of them made a cassette tape of someone else's music album? What mechanisms are in place--or could be put into place--to effectively convince these people that these acts are impermissible under the existing system?

The early Net users and the under-thirty crowd appear to have combined to create an interesting psychology on the Internet. The Internet community reacts with widespread disbelief when someone tries to assert that web browsing is an infringement,(72) that linking to a third party's materials is an infringement,(73) that forwarding an email to a mail list could be copyright infringement,(74) or that setting up a fan site could be an infringement.(75) Conceivably, the Internet community could be educated to understand why these actions implicate copyright rights, but changing the state of the Internet to conform to expansive readings of the copyright law would cause major upheaval. Furthermore, the logistics involved in trying to police these "micro-infringements" are daunting, and perhaps not efficient from a social cost versus social benefit standpoint.(76) Indeed, such an approach could ultimately prove economically counterproductive for intellectual property owners as well.(77)

More generally, the combination of the Internet culture and the general effect of technological evolution may be affecting our collective attitudes toward intellectual property. We have become a culture largely comfortable with serial micro-infringements. Generally, we want to respect other people's intellectual property rights, but we also want to run our lives in a way that ultimately results in numerous minor, almost trivial, but still theoretically actionable infringements.(78) The effect of trying to try to apply copyright laws (or worse, to try to strengthen them) to overcome this attitude would likely be regressive.

C. Conditioning to Expect Freebies

Because so many intellectual property owners are giving away valuable intellectual property for free, users are becoming conditioned to expect free intellectual property everywhere they go. In this environment, users become very reluctant to pay for intellectual property, since they know that free substitutes are likely to be available elsewhere. Even minor non-cash impediments, such as required registration forms, may be sufficient to drive users away. This conditioning makes it increasingly difficult for intellectual property owners to charge users directly for intellectual property.

VI. TECHNOLOGIES AND METHODS FOR CONTROLLING INTELLECTUAL PROPERTY

This section analyzes existing technological tools and other methods that enable intellectual property owners to protect their property. Technology will by necessity play an essential role in the controlled distribution of intellectual property on the Internet, despite the fact that many categories of intellectual property will be made available to consumers free of charge. Technology will help support revenue-producing markets in those categories of intellectual property that are not going to be freely given away, and it may also help those intellectual property owners who desire attribution.

Some people believe that the availability of the technologies described in this section will lead to the development of a micropayment economy, where even minor uses of intellectual property will result in micropayments to the intellectual property owners. In addition to this result being unlikely for the reasons described in part IV, micropayments raise other difficult issues. In particular, the transaction costs of micropayments can be relatively large--and any customer support is likely to be too costly to provide.(79)

Clearly no single technology or method can prevent all forms of infringement. However, it is both theoretically and practically possible that a combination of technologies and other methods will provide significant protection against unwanted infringement throughout the productive life of the intellectual property. By setting up impediments to infringement, the intellectual property owner can conform the behavior of those who are unwilling to invest the extra effort to infringe. Furthermore, while the pirates will have plenty of incentive to defeat the technology, "technology does tend to favor the good guys because the good guys are better funded."(80)

A. Pre-Infringement

This section describes technologies and methods that copyright owners may put into place before distributing their intellectual property to control or inhibit infringement of their works.

1. Limited functionality

Under this approach, intellectual property owners provide a copy of the work which is functionally limited. This approach provides one way to technically implement the "try before you buy" and "sell the upgrades" business models. For example, software creators can distribute software that cannot print or save. Under a slightly different approach, a software vendor can distribute "buggy" software, such as beta versions. While buggy software gives people the opportunity to use and become familiar with it, buggy software also induces those who desire stable software to purchase it. As a last example, database providers or other vendors of large pieces of intellectual property can deliver the content in small chunks, making it difficult to compile the complete work.(81)

2. Date bomb

Analogous to the limited functionality approach, under this approach the intellectual property owner distributes fully functional intellectual property but locks off access at a pre-specified date.(82) Under a variant of this approach, the vendor can lock off access after a certain number of uses (i.e., after viewing the file 10 times, the file may no longer be viewed).

3. Copy Protection

Under this approach, the vendor limits the number of times a file can be copied. Copy protection was standard in the 1980s, but it fell into disfavor largely because consumers resented the inconvenience and because copy protection was relatively easy to break.(83) While users are unlikely to be significantly more

responsive to copy protection schemes now, copy protection is currently being used in certain situations.(84) For example, a creator can save a file in Adobe Acrobat's PDF format in a manner that prevents others from making copies, either directly or by such indirect means as printing the screen or copying the text displayed on the screen.(85) While this form of copy protection is probably not "hack-proof," it is sufficient to inhibit the vast majority of users from copying files.(86)

4. Encryption Envelopes

Encryption envelopes are software devices which encrypt intellectual property in such a way that access can be obtained only by using the proper key.(87) These devices are often referred to by IBM's trademark name "cryptolopes." Creators can protect their works by distributing files in cryptolopes and requiring users to pay for keys that remove the work from the envelope.

5. Contracts

Contracts are an underrated pre-infringement control. When properly formed, contracts enable intellectual property owners to restrict the use of their intellectual property in excess of the rights granted under copyright laws.(88) An unresolved debate continues about the extent to which on-line shrinkwrap contracts (sometimes referred to as "clickthrough agreements") are enforceable.(89) If such agreements are enforceable, intellectual property owners may choose to rely heavily on contract law to control the use of their intellectual property.

B. Metering

This section describes technologies and methods that intellectual property owners can use to ensure payment prior to or at the time of a consumer's use of the intellectual property.

1. Access codes

Many of the devices described in the pre-infringement section can be coupled with "access code" devices. These devices permit users "unlock" protective mechanisms embedded in intellectual properties themselves, such as date bombs or functional limitations. This method allows the intellectual property owner to meter usage of the intellectual property, either by unlocking the intellectual property for a one-time license fee or by requiring periodic procurement of access codes.

2. Rights-Management Envelopes

As with encryption envelopes, the creator places intellectual property inside special software envelopes. However, under this approach the envelope periodically communicates with a home base to implement the business parameters imposed by the intellectual property owner. For example, Wave Interactive Networks <http://www. winhome.com/> provides a system which allows publishers to encrypt a file as a .wxn file, which when activated causes the Wave plug-in to debit the user's account maintained at Wave's website.(90)

3. Hardware Devices

Hardware device approaches require the user to acquire and install the requisite hardware device. For example, using a debit card approach, the user purchases a debit card that is pre-loaded with a certain amount of value. After installation, the debit card is debited automatically as the user consumes the intellectual property. In a "superdistribution" approach, the hardware device meters the usage of intellectual property and automatically debits an account maintained at a central base.(91)

In this way, even if the recipient has received a copy forwarded from a third party, the hardware device can ensure payment to the intellectual property owner.

4. Downloadable Executables

Downloadable executables, such as Java applets and ActiveX scripts, are pieces of code which download from the server to the client on a "use and discard" basis. In other words, the executable runs during a particular session but will be flushed from RAM at the end of the session. These executables can be metered out because they need to be downloaded each session.

5. Centralized Computing

Under this approach, all of the executables, other than a user interface on the client side, remain at the server. Therefore, the user's computer must establish contact with the server each time the executable is used, allowing the central computer to meter access. Centralized computing is actually the old "timeshare" model used in the early days of computing, when the client's processing power was so weak that centralizing

processing power at the server level was more efficient.

6. Digital Certificates

In the digital signature context, a certification authority issues to a user an electronic file (a "digital certificate") which identifies the user as the owner of a public key. However, digital certificates can be used to certify more information than mere identity. For example, they can be used to identify rights associated with a particular person. In these ways, vendors can use digital certificates to control access to system resources, including intellectual property files, by making files available to users who can provide a digital certificate with specified rights (such access, downloading, use, etc., including time limits). A user would obtain the digital certificate from either the vendor or a third party.

7. Copyright Clearinghouses

Under this approach, intellectual property owners would vest "clearinghouses" with the ability to license usage of their intellectual property. A user would pay a license fee to such a clearinghouse to obtain rights to the intellectual property. Copyright clearinghouses currently exist for music-related intellectual property,(92)although these are products of statutory compulsory licensing.(93) No similar comprehensive mechanisms have developed for other forms of intellectual property,(94) despite some long-standing attempts to do so(95) and the widely recognized benefits of having such a scheme in place. As a result, some technological efforts are being made to include copyright management information in all electronic files so that contact information for procuring copyright permissions will always be available.(96)

8. Sale of Physical Copies

As anachronistic as it may sound, selling physical copies of intellectual property remains a highly effective method of metering the usage of intellectual property. While the electronic distribution of intellectual property has many advantages, numerous advantages to purchasing physical copies of works available on the Internet still remain. First, many people still prefer reading physical copies over reading electronic copies. Second, obtaining a mass-produced physical copy rather than printing out the electronic copy may be beneficial from a cost or quality standpoint. Third, in the case of large electronic files, obtaining a physical copy may be more time-effective or convenient than downloading the electronic copy. Fourth, the consumer may use devices that have been optimized for use with physical copies, providing results that exceed the results available from using the downloaded electronic copy. Therefore, we should expect that certain categories of intellectual property will continue to be demanded in physical versions.

C. Post-Infringement

This section describes technologies and methods that creators can use to identify infringements and thus enhance enforcement of intellectual property rights.

1. Agents

Agents are programs that can implement specified commands automatically. Intellectual property owners can used agents to search the public spaces of the Internet to find infringing copies.(97) While agent technology is still being developed and refined, even today creators can perform a relatively powerful set of searches using full-text search engines such as HotBot <http://www.hotbot.com/> and Alta Vista <http://www.altavista.digital.com/>.

2. Steganography

Steganography, as applied to electronic files, refers to the process of hiding information in files in such a way that the hidden information is not easily detected by the user. Intellectual property owners can use steganography in a number of different ways on the Internet. One approach is to insert into the file a "digital watermark" which can be used to prove that an infringing file was the creation of the intellectual property owner and not the pirate.(98) The owner of the work could also store copyright management information using this technology. Another approach is to encode a unique serial number into each authorized copy of the file, enabling the owner to trace infringing copies to a particular source.(99)

3. Copyright Litigation

Copyright litigation is a powerful tool for enforcing intellectual property rights, one that should not be overlooked. While not every infringement will be the subject of litigation, the threat of litigation helps keep large pirate operations in check.(100) Copyright litigation not only helps the intellectual property owner obtain relief for specific acts of infringement, it publicly warns others of the dangers of infringement. Indeed, a number of intellectual property owners have had well-publicized successes enforcing their copyrights against on-line infringers.(101)

D. Additional Problems Under Copyright Law Possibly Solvable by Technology

This section discusses some additional complex issues under U.S. copyright law that are not fully addressed by the technologies and methods described in parts VI.A-C, *supra*, but are still addressable by technology. In particular, linking and caching are both techniques used in the normal functioning of the Internet, yet their permissibility under U.S. copyright law is unclear.

When the technologies available for controlling linking and caching are combined with the technologies and methods described in parts VI.A-C, *supra*, the mosaic of the overall set of protection technologies and methods available to intellectual property owners becomes clearer. This clarity will lead to the question, discussed in part VI.E, infra, of whether situations exist the intellectual property owner should have the obligation--if he or she wants to exercise it--to prevent users from infringing before the owner is given the right to claim infringement.

1. Linking

Hypertext linking is one of the blessings of the Internet, but its application has proven problematic. Most copyright experts generally believe that linking should not lead to copyright liability,(102) because the mechanical operation of the hypertext link does not implicate one of the exclusive rights of copyright owners; a hypertext-linked URL is merely an instruction which is loaded into the user's browser software, and the browser software does all of the work from there. As a result, the server providing the hypertext link never makes a copy or otherwise processes any of the data from the linked site.(103)

While the plain language of the copyright statute suggests the above conclusion, commentators, to ensure that linking is not copyright infringement, have argued that uploading intellectual property to the Internet grants an "implied license"(104) to link. Alternatively, linking might be considered fair use.

Of course, given the alternative business models discussed earlier, in many cases Internet sites eagerly seek out linking as an entree to generate ancillary values. In fact, a nascent business of providing links has developed.(105) However, if an Internet site does desire to keep others from linking to some or all of its pages, a number of technologies are available to inhibit linking:

- The system operator (the "sysop") can make the page a "dynamic" page by building the page only when the user causes the execution of a program resident on the server. This prevents linking because dynamic pages have no fixed reference point to which to link. This technique, while effective, is also currently somewhat expensive. Alternatively, the low-technology approach is for the sysop to manually change the page's URL periodically, so that any links made to the page will become ineffective.
- If the sysop desires to prevent a specific site from linking to a page, the sysop may code the page in such a way that it refuses browsers who access the site from the forbidden linking site.(106)
- In the case of automatic linking performed by robots and spiders (such as those used by the search engines), the sysop may load information into the header of the page that instructs the robots and spiders not to index the page.
- The page can be password protected, although this practice inhibits the page's free accessibility to people browsing the Internet.
- To address the problem of unattributed graphics being incorporated into pages on a remote system, the graphic may contain a program that automatically causes a notice to appear to users who access it that the graphic is the copyrighted work of the intellectual property owner.(107)

2. Caching

Caching is a loosely used term that generally refers to the process of making an extra copy of a file or set of files for more convenient retrieval. On the Internet, caching of third party files can occur both locally on the user's client computer (either in RAM or on the hard drive) or at the server level (called "proxy caching"). When a user requests a file that has been cached, the browser will deliver the file from the cache rather than retrieving a fresh copy over the Internet.

Although different concepts, similar issues to caching arise with mirroring (establishing an identical copy of an Internet site on a different server), archiving (providing an historical repository for information, such as with newsgroups and mail lists, where the proceedings would otherwise be evanescent), and full-text indexing (the copying of a document for loading into a full text or nearly full-text database which is searchable for key words or concepts).

Caching is an integral part of the Internet's operation, in part because it speeds the user's access to files and in part because it reduces the infrastructure required for operation of the Internet (by reducing the number of files that must be transferred using the infrastructure). Without caching, our already taxed infrastructure

would be even more clogged, to the point where it may become unworkable. As a result, a number of serious business plans have been predicated on using caching.(108)

However, caching could cause harm because the copies in the cache are not necessarily the most current and up-to-date copies.(109)For example, users relying on the cached copy may unwittingly use out-of-date material; similarly, harms such as defamation or infringement that existed on the original page may propagate for years until flushed from each cache where they have been replicated.(110) Also, since caching is an infringement under a literal reading of U.S. copyright law, either caching must be the subject of an implied license or fair use defense or it is (at least theoretically) actionable.

Internet sites can deploy a number of technologies to restrict or prevent caching:

- Sysops can make the page a "dynamic" page by building the page only when the user causes the execution of a program resident on the server. As in the case of linking, this solution may be expensive.
- Sysops may place information on the page's header which tells the party trying to cache the page when to replace the copy in the cache with a new copy (this is called an "expiry header"). In the case of a sysop who does not want the page cached at all, the sysop merely sets the expiry date as a date before the date on which the information is loaded. Unfortunately, no technology standards presently exist under which caching entities can read and manage this process automatically, so a sysop's instructions may well be ignored or not processed.
- The page can be password protected, although again this inhibits the page's free accessibility to Internet browsers.

Finally, parties trying to establish caches have an incentive to deploy software that automatically updates the cache every time the cached page changes. While this practice solves many of the problems, it leaves control of the process with the entity doing the caching rather than with the website being cached.

E. Is Technology a Substitute for Copyright Law?

Many on the Internet implicitly believe that the failure of an intellectual property owner to use available technology to prevent infringement controls grants to all comers an implied license to infringe. This attitude is seen most often in the arguments raised against copyright infringement for linking and caching. However, based on all of the possible technological controls available to intellectual property owners as described in this part VI, the "use technology or accept infringement" argument might be expanded to apply to all types of infringement, going far beyond just linking and caching.

In some ways, this argument is unprecedented. No other situation come to mind where a copyright owner's failure to use technological protective controls has the effect of diminishing their rights under copyright law.(111) Why should the Internet create a new paradigm?

On the other hand, the normal functioning of the Internet is predicated on multiple infringements of copyright rights. If we want the Internet to work as it currently operates and as it can operate in the future, we must reduce the chilling effect of the threat of copyright litigation by changing the rules (or interpreting them differently) or placing some burden on intellectual property owners to "opt out" of the system by deploying technology controls.

Given that many intellectual property owners' business models are based on encouraging "infringement" by users, and that many users believe (innocently but mistakenly) that intellectual property found on the Internet is free for the taking, a trend is emerging toward increasing the burden placed on intellectual property owners to adopt technology controls rather than relying on copyright infringement litigation. Interestingly, this trend is incompatible with the efforts of those seeking to increase the scope of the copyright laws.(112)

VII. CONCLUSION

Even though many of this article's specifics will be out-of-date soon after it is published, its general conclusions should have lasting relevancy to the policies of future U.S. copyright law. This article has marshaled evidence to support the following conclusions:

- The creation and dissemination of intellectual property, both on the Internet and more generally, seems highly robust despite all of the threats.
- The economics of the Internet dictate that, in many cases, businesses must find a way to generate revenues without charging users for intellectual property.
- A wide variety of sustainable business models permit businesses to accomplish that end.
- Users are becoming increasingly unwilling to pay directly for intellectual property.
- The elimination of all infringements is an impossible and possibly undesirable goal.

- A cadre of entrepreneurs and existing companies are introducing a wide variety of technologies that intellectual property owners can use to manage the process of infringements.
- The perception is increasing that intellectual property owners should be required to use the available technological tools rather than relying on the threat of litigation over micro-infringements.

As a practical reality of these conclusions, the real battle between intellectual property owners and Internet users is being waged using the business models and technological tools available to intellectual property owners. Combined with the trends in sociological beliefs about the Internet, the business models and technological tools will evolve over time to make copyright law increasingly less important as a tool for conforming behavior on the Internet.

Concluding that copyright law's unimportance on the Internet suggests that copyright law should be abolished generally would be inaccurate. The fact that the existing copyright laws may have no effect on the way creators and consumers operate on the Internet does not mean that we no longer need these laws. Existing copyright laws are critically important to the world of physical space.(113) This holds true even though the Internet may become the preeminent vehicle for the dissemination of intellectual property.

However, except in the possible case of attribution rights, no new laws designed to increase the rights of intellectual property owners on the Internet are currently needed. Any such legislation would most likely destroy the delicate balance being struck in the marketplace right now. Furthermore, any anomaly in the existing laws is likely to be resolved by technological and business innovation, which is occurring at a dizzying rate.

We live in an energizing information age, where we are beginning to realize many of yesterday's dreams about information exchange on a global scale. We should facilitate this environment by letting the marketplace reach its own equilibrium. We can do this best by pursuing legislation which regulates only the most extreme behavior, leaving the rest of the spectrum of behavior for marketplace solutions.

FOOTNOTES

© 1997 Cooley Godward L.L.P.

+.UCLA B.A. 1988, M.B.A., J.D. 1994. The author is an attorney practicing cyberspace law with Cooley Godward L.L.P. Palo Alto, California, and is also an adjunct professor of Cyberspace Law at the Santa Clara University School of Law. The author wishes to extend special thanks to: the members of the CNI-COPYRIGHT mail list, whose contributions to an initial draft of this paper were invaluable to refining his interest in this topic; Stephen Paternot and Todd Krizelman of Cooley Godward's client WebGenesis, whose leading edge business models have led to numerous insights; and Lisa Sanger, a constant source of inspiration. The author also appreciates the comments to prepublication drafts of this paper given by Brad Biddle, John Cummerford, Viraj Jha, Michael Lean, Mark Lemley, Shawn Molodow, Ross Mutton, Mark Perkins, Eric Reifschneider, Lisa Sanger, Paul Startz, and Shelly Warwick.

The views expressed in this article are the author's own and do not necessarily reflect those of Cooley Godward or its clients. Cooley Godward represents some of the companies referenced in this article.

The author can be reached at schlachtere@cooley.com.

[BTLJ Web Editor's note: After reading a footnote, use your browser's "back" button to return to the main text.]

1. Ithiel de Sola Pool, Technologies of Freedom 214 (1983).

2. *See* U.S. Dep't of Commerce, Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property 10-11 (1995) [hereinafter NII White Paper], *available at* http://www.uspto.gov/web/offices/com/doc/ipnii; Ken Kay & Steve Metalitz, *Copyright Act Needs Digital Expansion*, Legal Times, Apr. 8, 1996 http://www.cic.org/clip5.html; Mark Stefik, *Trusted Systems*, Sci. Am., Mar. 1997 http://www.sciam.com/0397issue/0397stefik.html; ("Uncontrolled copying has shifted the balance in the social contract between creators and consumers of digital works to the extent that most publishers and authors do not release their best work in digital form.").

[Throughout this article, websites are referenced as both primary and secondary sources. Unless otherwise noted, all websites were verified on May 1, 1995.]

3. NII White Paper, *supra* note 2, at 17. However, criticism of the NII White Paper has been widespread, with commentators arguing that its proposed changes are not minor. *See, e.g.*, Pamela Samuelson, *The*

Copyright Grab, Wired, Jan. 1996, at 134, *available at* <http://www.hotwired.com/wired/4.01/features/white.paper.html>; Digital Future Coalition <http://www.ari.net/dfc>.

Although this article focuses on the Internet, much of the analysis applies with equal force to other networks such as BBSs and on-line services.

4. *See* John Perry Barlow, *Selling Wine Without Bottles: the Economy of Mind on the Global Net* (a.k.a. *The Economy of Ideas*), Wired, Mar. 1994, at 85, *available at* <http://www.hotwired.com/wired/2.03/features/economy.ideas.html> ("Intellectual property law cannot be patched, retrofitted, or expanded to contain digitized expression any more than real estate law might be revised to cover the allocation of broadcasting spectrum...."); Esther Dyson, *Intellectual Value,* Wired, July 1995, at 136, *available at* <http://www.hotwired.com/wired/3.07/features/dyson.html>.

5. This article discusses only U.S. copyright law, although other copyright law schemes are similarly worthy of analysis.

6. *See, e.g.,* NII White Paper, *supra* note 2, at 19-147; Terry Carroll, *Frequently Asked Questions About Copyright*, version 1.1.3, January 6, 1994 <http://www.eff.org/pub/ intellectual_property/copyright.faq>.

7. U.S. Const. art. 1, sec. 8, cl. 8.

8. 17 U.S.C. 101 et seq. (1994).

9. *See* Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 340 (1991), *available at* <http://www.seamless.com/rcl/feist.html>.

10. 17 U.S.C. sec. 106 (1994).

11. *Id.* sec. 302.

12. *Id.* sec. 107.

13. *See* Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 449-50 (1984).

14. *See* NII White Paper, *supra* note 2, at 79.

15. Lance Rose, *The Emperor's Clothes Still Fit Just Fine*, Wired, Feb. 1995, at 103, 104, *available at* <http://www.hotwired.com/wired/3.02/departments/rose.if.html>; *See* Philip E. Ross, *Cops Versus Robbers in Cyberspace*, Forbes, Sept. 9, 1996, at 134, 137, *available at* <http://www.forbes.com/forbes/090996/5806134a.htm> (noting that "[intellectual] property owners rely heavily on old-fashioned methods: police raids, lawsuits and tip-offs," all of which become more likely as the size of the venture increases).

16. *See* Jessica Litman, *The Exclusive Right to Read*, 13 Cardozo Arts & Ent. L.J. 29, at 50-51 (1994), *available at* <http://yu1.yu.edu:80/csl/journals/aelj/articles/13-1/ litman.html> ("The current copyright statute has proved to be remarkably education-resistant.... [O]ur current copyright statute could not be taught in elementary school, because elementary school students couldn't understand it. Indeed, their teachers couldn't understand it. Copyright lawyers don't understand it.").

17. *See* Steve G. Steinberg, *Seek and Ye Shall Find (Maybe)*, Wired, May 1996, at 108, *available at* <http://www.hotwired.com/wired/4.05/features/indexweb.html> (noting that "at its current growth rate, the Web will contain more words than the giant Lexis-Nexis database by [summer 1996], and more than today's Library of Congress by the end of 1998").

18. *See* Netbot <http://www.netbot.com/>. For example, the Internet provides numerous "agents" for buying music CDs. These agents search the available pricing databases on the Internet and deliver a comprehensive set of results, allowing customers to easily compare prices and, presumably, choose the lowest. *See, e.g.,* BargainFinder Agent <http://bf.cstar.ac.com/bf/>.

19. *See* part III.B *supra*. In part, transaction costs are limited due to current market conditions of pricing for access that does not vary with usage. There has been much discussion suggesting that per-byte or per-unit pricing will be required because of the problems inherent in a system where users can get unlimited use of the scarce resources of the Internet without paying marginal costs. *See* Jeffrey K. MacKie-Mason & Hal R. Varian, *Economic FAQs About the Internet* (June 1995) <http://www.spp.umich.edu/ipps/papers/info-nets/Economic_FAQs/FAQs/FAQs.html>.

20. A producer will continue to produce so long as the marginal revenue from an additional unit of output is

greater the marginal cost of such output, since the difference represents a contribution towards fixed costs. In an efficient market, the party with the lowest marginal cost sets the price, since it is able to undercut its competitors' prices and therefore win customers.

21.In the long run, all costs are variable costs. However, in the short run, costs that cannot be varied easily are fixed costs. Therefore, costs such as salaries, hardware and software expenses and contractual commitments for Internet service are all fixed costs in the short run.

22.*See, e.g.,* James Gleick, *I'll Take the Money, Thanks*, New York Times Magazine, Aug. 4, 1996, at 16, *available at* <http://www.around.com/copyright.html>.

23.*See* Hal R. Varian, *Differential Pricing and Efficiency* (June 1996) <http://alfred.sims.berkeley.edu/Different/different.html> (arguing that it is optimal for intellectual property to be offered on a price-discriminated basis). Price discrimination is tricky because it requires careful definition of the product being price-discriminated. If the business model adopted by an Internet company is to provide free intellectual property as an inducement to sell other goods or services, is the "product" the intellectual property or the package of intellectual property plus the ancillary goods or services?

24.*See* Robert Metz, *Shaking the Money Tree* (Nov. 4, 1996) <http://www.talks.com/ library/rm110496.html>.

25.It is generally believed that few, if any, Internet businesses are currently making a profit. *See, e.g.*, Kathy Rebello, *Making Money on the Net*, Bus. Week, Sept. 27, 1996, at 104, *available at* <http://www.businessweek.com/1996/39/b34941.htm> (indicating that Internet businesses losing money outnumber moneymakers two to one); *See* Jeff Moad, *Web Shakeout*, PC Week, July 15, 1996, at E1, *available at* <http://www8.zdnet.com/pcweek/ExecConnect/0715/15emain.html> (describing a number of high-profile failures of Internet businesses). This limited empirical evidence does not yet prove that the Internet will provide insufficient profits to induce the creation of intellectual property. The Internet is far from mature, either as a commercial environment or in terms of the predictability its technical or legal framework. Further, in most industries, significant upfront investments must be made before profits accrue--and most Internet businesses are less than 3 years old. Instead, the high stock valuations of many Internet companies indicates that many investors forecast significant future profits.

26.*See, e.g.,* Juno On-line <http://www.juno.com/> and Hotmail <http:// www.hotmail.com/>. Other companies, such as Cyber FreeWay <http://cyberfreeway.net/> and @bigger.net <http://bigger.net/> are offering lifetime email accounts for a low one-time fee. However, Freemark, one of the early entrants in this arena, has already gone defunct.

27.*See, e.g.,* Pointcast Network <http://www.pointcast.com/>, Freeloader <http:// www.freeloader.com/> and Mercury Mail <http://www.merc.com/>.

28.*See, e.g.,* HotWired <http://www.hotwired.com/> and C|Net <http://www.cnet.com/>.

29.*See, e.g.,* HotBot <http://www.hotbot.com/>, Yahoo! <http://www.yahoo.com/>, Excite <http://www.excite.com/>, InfoSeek <http://www.infoSeek.com/>, Switchboard <http://www.switchboard.com>, Four11 <http://www.four11.com/> and BigBook <http://www.bigbook.com/>.

30.*See* Lauren Gibbons Paul, *Web Rewards Wait Only for the Patient*, PC Week, July 15, 1996, at E4, *available at* <http://www8.zdnet.com/pcweek/archive/1328/ pcwk0007.htm> (suggesting that content sites should not expect to break even before the year 2000); Rosalind Resnick, *Follow the Money*, Internet World, May 1996, at 34, 34-36 [hereinafter Resnick, *Follow the Money*], *available at* <http://www.iw.com/1996/05/ money.html> (noting that advertising revenue is heavily concentrated among a small number of sites, leaving few advertising dollars for other sites); *See also* Hunter Madsen, *Reclaim the Deadzone*, Wired, Dec. 1996, at 206, 212, *available at* <http://www.wired.com/ wired/4.12/esmadsen.html> (describing how the limited real estate for banner advertisements suggests that banner advertisements will be insufficient to support Web publishing). Web advertisement revenues were $71.7 million in the first six months of 1996, although they are expected to increase to $5 billion in 2000. Rebello, *supra* note 25, at 107.

31.*See* Zachary Schiller, *For More About Tide, Click Here*, Bus. Week, June 3, 1996, at 44, *available at* <http://www.businessweek.com/1996/23/b3478129.htm> (describing how Procter & Gamble, America's largest advertiser, has attempted to pay based solely on click-through rates, not page impressions).

32.*See* Craig R. Evans, *The Web's REAL Opportunity--Advertising!*, Elec. Retailing, Sept./Oct. 1996, at 6 (describing a survey of Web users indicating that 46% of those who used the Web to research products and services went on to buy the product at retail).

33.*See* Rosalind Resnick, *AdTech '96: Is Banner Advertising Dead?*, Interactive Publ'g Alert, July 1, 1996 <http://www.netcreations.com/ipa/banners.html> [hereinafter Resnick, *Banner Advertising*] (describing "sponsored content," "targeted direct mail" and "pay-per-use" advertising strategies).

34.Madsen, *supra* note 30, at 220.

35.In another example, IBM makes the full text of patents issued to it since 1971 available for free on its website. IBM's motivation is, in part, to reinforce the message that IBM has received more patents than anyone else for the past several years. *See* IBM Patent Server <http://patent.womplex.ibm.com/>.

36.Resnick, *Banner Advertising*, *supra* note 33.

37.*See* Margie Wylie, *Can Copyright Survive the Digital Age? Should It?*, Digital Media: A Seybold Report, July 3, 1995 (on file with author) ("'Some of the more popular spreadsheet and wordprocessing programs were greatly aided by being ripped off to a certain degree.' It let people use them enough that they were convinced it was worth the money to buy a legitimate copy, with documentation, support and upgrades." (quoting R.W. Lucky of Bellcore Labs)).

38.This model is exemplified by the long-standing "shareware" industry. *See, e.g.,* McAfee, <http://www.mcafee.com/>, which makes anti-virus shareware software, and Netscape <http://www.netscape.com/>, which gives its browser away as shareware. Id Software, the makers of Doom II, a popular (and violent) computer game, took a slightly different approach--they gave away the first 3 basic "levels" of the Doom II dungeon; the other 47 levels were made available for a charge.

39.Numerous pornography sites on the Internet offer a few free photos for browsing as a teaser to purchasing access to the remaining database of photos. *See generally* <http:www.yahoo.com/Society_and_Culture/Sexuality/>.

40.*See, e.g.,* the Wall Street Journal Interactive Edition <http://www.wsj.com/>, which offers a free two-week trial subscription.

41.*See* Paulina Borsook, *Steal This Article*, Upside, Mar. 1996 at 80, 88 [hereinafter Borsook, *Steal This Article*], *available at* <http://www.upside.com/texis/archive/ search/article.html?UID=9603011002> (describing how music groups have a love/hate relationship with their underground fans, knowing that infringement by the underground is often a way to expand their fan base). Spectrum Press <http://users.aol.com/ specpress/free.htm> gives away samples of short stories and novels that it sells in electronic form delivered on floppy disks. *But see id.* ("'You can upgrade software, not music.'" (quoting Judith Saffer, in house attorney for BMI)).

42.*See* Caryn Gillooly, *Cabletron's Unbeatable Price Plan*, Info. Week, July 24, 1995, at 28 (describing how Cabletron was giving away its Spectrum software, worth $20,000, as an entree to sell its other network management products).

43.Rose Aguilar, *Digital to Market Alta Vista*, Mar. 29, 1996 <http:// www.news.com/News/Item/0,4,1005,00.html>.

44.This model may explain why companies tolerate unauthorized fan sites. *Cf.* Constance Sommer, *Film Rights Falling Through the Net*, San Jose Mercury News, Dec. 10, 1996, at 10E (referring to Disney's laissez-faire attitude toward on-line fan sites).

45.*See* Paulina Borsook, *Music Lessons*, Upside, Mar. 1996 at 84, [hereinafter Borsook, *Music Lessons*] (describing how music companies can add value to free on-line music sufficient to induce purchases of CDs through better packaging, thicker CD booklets, and accompanying video).

46.A "cookie" is a file on the user's hard drive where websites may store user-specific information. Most browser software programs support the use of the cookie.

47.*See, e.g.,* CyberGold <www.cybergold.com> (a service which will pay users to read advertisements sent to them based on their articulated preferences).

48.*Cf.* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 <http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html> (discussing the protection of individuals with regard to the processing of personal data and the free movement of such data).

49.*See* Rebello, *supra* note 25, at 106 ("'[Community-building] is the secret weapon of an electronic merchant.'" (quoting Amazon.com founder Jeff Bezos)). *See generally* Arthur Armstrong & John Hagel III, *The Real Value of On-Line Communities*, Harv. Bus. Rev., May-June 1996, at 134.

50.*See* Neil Gross & Peter McCoy, *The Technology Paradox*, Business Week, Mar. 6, 1995, at 76, 80 (describing how giving intellectual property away for free can build mindshare in the coming "attention economy").

51.*Id.* at 77.

52.17 U.S.C. sec. 106A applies only to "visual works," which include paintings, drawings, prints or sculptures in a limited edition of less than 200 copies which are signed and consecutively numbered, or a still photographic image which is a single copy signed by the author or is a limited edition of less than 200 copies signed and consecutively numbered. *Id.* sec. 101. While it theoretically possible for a work existing on the Internet to be categorized as such, this possibility is highly remote.

53.None of the six exclusive rights of copyright have been interpreted to require attribution. *See* Mark A. Lemley, *Rights of Attribution and Integrity in On-line Communications*, 1995 J. On-line L. art. 2 <http://warthog.cc.wm.edu/law/publications/ jol/lemley.html>.

54.*See* John S. Erickson, *Open Commerce through Enhanced Attribution* (1996) <http://www.netrights.com/EnhancedAttribution.html>; *cf.* Borsook, *Music Lessons*, *supra* note 44, at 84 (describing how a musical group used the name of a Japanese character for one of the group's songs; the litigation over the use of the name was amicably settled when the group pointed out that the character owner could not buy the kind of free advertising it had received).

Some of the business models, such as advertising, may require the attribution to occur only on the site where the advertising is located. Therefore, not every business using cross-subsidization will necessarily encourage widespread infringement.

55.NII White Paper, *supra* note 2, at 235. See also Julie A. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 Berkeley Tech. L.J. 161 (1997) [hereinafter Cohen, *Copyright Management Systems*] (discussing policies prohibiting alteration of copyright management information).

56.*Id.* The reference to terms and conditions of use may be problematic because it suggests that owners can unilaterally impose "contract" terms on all consumers of the file. *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace,* 28 Conn. L. Rev. 981 (1996) [hereinafter Cohen, *Right to Read Anonymously*]. While this unilateral contract approach might be the right result, as found in ProCD v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996), *available at* <http://www.kentlaw.edu/7circuit/1996/jun/96-1139.htm>, no consensus currently exists that the *federal* government should be dictating that licensors should be permitted to unilaterally impose contract terms on licensees. *See* U.C.C. *proposed* Article 2B (Mar. 21, 1997 draft) <http://www.lawlib.uh.edu/ucc2b/> (a controversial attempt to develop model *state* legislation permitting increased ease in the formation of unilateral contracts by licensors); *See also* Maureen O'Rourke, *Copyright Preemption After the ProCD Case: A Market-Based Approach*, 12 Berkeley Tech. L.J. 53, 71 (1997). This issue is particularly important because presumably the licensor-imposed terms will exceed the licensor's rights under copyright law (otherwise, why would they need to impose them?). However, terms and conditions would be less problematic if they were merely grants of licensor's copyright rights (i.e., "you may use this material for any noncommercial use").

57.*See* World Intellectual Property Organization, Diplomatic Conference on Certain Copyright and Neighboring Rights Questions, WIPO Copyright Treaty (Dec. 23, 1996) <http://www.wipo.org/eng/diplconf/distrib/94dc.htm>; World Intellectual Property Organization, Diplomatic Conference on Certain Copyright and Neighboring Rights Questions, WIPO Performances and Phonograms Treaty (Dec. 23, 1996) <http://www.wipo.org/eng/diplconf/distrib/95dc.htm>. *See also* Cohen, *Copyright Management Systems*, *supra*, note 56 at 161, 165-69.

58.Prof. Samuelson also notes that the proposal could protect devices incorporated into files that effectively report on users' behavior, raising potentially serious privacy concerns. Samuelson, *supra* note 3, at 188; *See also* Cohen, *Right to Read Anonymously*, *supra* note 56.

59.The HTML command "img src," followed by a URL, instructs the user's browser software to access the file contained at the referenced URL and to incorporate that file into the page displayed to the user. The user will see the file displayed on the page, but the user will not see the site from which the file originated, nor will the linking site store a copy of the linked-to file on its server. Issues related to linking are discussed in part VI.D.1, *infra*.

60.*Cf.* CompuServe, Inc. v. Cyber Promotions, Inc., 1997 U.S. Dist. LEXIS (S.D. Ohio Feb. 3, 1997), *available at* <http://www.bna.com/e-law/cases/compus1.html> (discussing how when a mass email sender was notified by CompuServe that their "junk" email was no longer welcome, the sender's continued sending of mass emails was a trespass to chattels; however, notice "may be insufficiently communicated to potential third-party users when it is merely posted at some location on the network.").

61.*See, e.g.,* SavvySearch <http://williams.cs.colostate.edu:1969/>.

A recent case involving the use of "frames" raises similar issues which arise when one site engages in "free riding" on the efforts of other sites. *See* Washington Post Co. v. Totalnews, Inc. (complaint filed Feb. 20, 1997) <http://www.ljx.com/internet/complain.html>. However, Totalnews does provide attribution to the sites it frames.

62. *But see* Cohen, *Right to Read Anonymously*, *supra* note 56 (assuming that each intellectual property is unique to the point that owners are able to exercise monopoly powers sufficient to impose unfair terms on consumers seeking access to the work).

63. *See generally* Gross & McCoy, *supra* note 50 (describing the recurring phenomenon of valuable goods and services being given away for free, even where manufacturing and distribution have marginal costs).

64. Which categories these are is presently unclear, but presumably they will be categories lacking high fungibility between specific intellectual property outputs.

65. *See* Lance Rose, *Is Copyright Dead on the Net?*, Wired, Nov. 1993, at 112, *available at* <http://www.hotwired.com/wired/1.5/departments/idees.fortes/copyright.on.net.htm>(discussing various visions of what copyright law means on the Internet).

66. *See generally* Berne Convention for the Protection of Literary and Artistic Works (Paris Text 1971), sec. 6*bis* <http://www.law.cornell.edu/treaties/berne/6bis.html>.

67. *See* NII White Paper, *supra* note 2, at 146.

68. 17 U.S.C. sec. 106A (1994).

69. *See* Rose, *supra* note 15, at 104.

70. *See* Rebello, *supra* note 25, at 113-14.

71. *Cf.* Litman, *supra* note 16, at 34-35 ("Most of us can no longer spend even an hour without colliding with copyright law. Reading one's mail or picking up one's telephone messages these days requires many of us to commit acts that [the NII White Paper] now tells us ought to be viewed as unauthorized reproductions or transmissions.").

72. *See* NII White Paper, *supra* note 2, at 64-65.

73. *See* The Shetland Times Ltd v. Wills, Court of Sessions, Edinburgh, October 24, 1996 <http://www.shetland-news.co.uk/opinion.html> (a United Kingdom court enjoined one newspaper from hypertext linking to stories at a competing newspaper's website).

74. *See* Mitch Betts, *On-line Pay Per View*, ComputerWorld, June 5, 1995, at 58, *available at* <http://www.computerworld.com/search/AT-html/9506/950605SL22 rights.html> (citing a survey of 255 information systems professionals which indicating that 72% believed they "should be able to download on-line news articles and share them with as many people as they want").

75. For example, when Lucasfilms, the owner of Star Wars, contacted a dedicated fan who had established a Star Wars appreciation website regarding alleged infringements, the fan transcribed the conversation and posted the transcription on the website. After Lucasfilms was flooded "with angry emails, demanding to know how it could presume to assert such totalitarian control over a product some fans had woven into the very fabric of their lives," Lucasfilms backed down. Sommer, *supra* note 44, at 10E.

76. *See* Wylie, *supra* note 37 ("Copyright doesn't work today because people pay 100 percent of the time. It works because people pay often enough that intellectual property owners make a profit."); *cf.* Borsook, *supra* note 45, at 84 (noting that the music industry long ago accepted that it would lose 15-20% of its potential revenues to home copying).

77. A good example can be found in the movie studios' action against video cassette recorder manufacturers, Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984), where the studios' victory would have inhibited the development of an industry (video cassette rental) that generated $13 billion in revenues for the studios in 1993. *See Current Revenue of Target Markets*, Upside, Dec. 1994 at 18 (graph referencing a Yankee Group study); *cf.* Litman, *supra* note 16, at 46 ("Whenever we have discovered or enacted a copyright exception, an industry has grown up within its shelter.").

78. *The Property of the Mind*, Economist, July 27, 1996, at 57, 57. <http://www.economist.iconnet.net/issue/27-07-96/wbsf1.html>.

79. Tom Steinert-Threlkeld, *The Buck Starts Here*, Wired, August 1996 at 132, 134, *available at*

<http://www.wired.com/wired/4.08/features/nanobucks.html>.

80.Ross, *supra* note 15, at 137.

81.*Id.* Compare the approach used by Lexis in delivering cases on a screen-by-screen basis; compiling the full case by capturing each screen would be arduous.

82.*See, e.g.,* Release Software's SalesAgent <http://www.releasesoft.com/ sadiagram.html>.

83.Ross, *supra* note 15, at 136.

84.*Cf. id.* (describing how Macrovision "spoilers" are inserted into movies; the spoilers confuse VCRs and produce distorted versions of the movies if copied).

85.Maximized Software's SiteShield software <http://www.maximized.com/ products/siteshield/> encodes files in such a way that they may be browsed but not otherwise copied.

86."'Now, people say to themselves "Hey, let me take this for free," but with [Maximized Software's SiteShield], they'd have to decide to be trespassers.... People would have to put effort into stealing the images, and they'd know they were violating the copyright.'" Ross, *supra* note 15, at 139 (quoting Kenneth Spreitzer, president of Maximized Software).

87.*See* <http://www.cryptolope.ibm.com/wiacc.htm>; *See also* Digital Delivery's TitleBuilder <http://www.digitaldelivery.com/tbpage.html>; Portland Sotware's ZipLock <http://www.portsoft.com/ziplock.html>.

88.In some circumstances the enforcement of the contract will be limited because the contract provisions are preempted by copyright law. *See* Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 268-70 (5th Cir. 1988). *See generally* I. Trotter Hardy, *Contracts, Copyright and Preemption in a Digital World,* 1 Rich. J.L. & Tech. 2 (1995) <http://www.urich.edu/~jolt/v1i1/hardy.html>; *See also,* O'Rourke, *supra*, note 56.

89.*Cf.* ProCD v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996), *available at* <http://www.kentlaw.edu/7circuit/1996/jun/96-1139.htm> (holding that a shrinkwrap license, the functional equivalent of a "clickthrough" license, could constitute a properly formed contract); Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997) (following ProCD); U.C.C. *proposed* Article 2B (Mar. 21, 1997 draft) <http://www.lawlib.uh.edu/ucc2b/> (making it easier for licensors to form shrinkwrap agreements with end users).

90.*See* InterTrust <http://www.intertrust.com/products/flow.html> (describing the DigiBox envelope, which communicates with a clearinghouse based on business rules encapsulated in the envelope); Gary N. Griswold, *A Method for Protecting Copyright on Networks,* 1994 <http://www.cni.org/docs/ima.ip-workshop/www/Griswold.html> (describing a software envelope which requires periodic confirmation with a home base prior to permitting further access); Stefik, *supra* note 2 (describing protocols to permit the permanent transfer or temporary lending of files while holding the number of files to the number actually paid for).

91.Brad Cox, *Superdistribution*, Wired, Sept. 1994, at 89, *available at* <http://www.hotwired.com/wired/2.09/departments/idees.fortes/superdis.html>; *see* Infosafe Systems <http://www.infosafe.com/> (offering both a hardware system and a software-only system).

92.*See* ASCAP <http://www.ascap.com/ascap.html> and BMI <http://bmi.com/>.

93.17 U.S.C. secs. 115 (making and distributing phonorecords), 116 (public performances by means of coin-operated phonorecord players ("juke boxes").

94.The Copyright Clearance Center <http://www.copyright.com/> can grant licenses to reproduce 1.75 million documents--an impressive number, but clearly far short of the overall set of works subject to copyright available in the world.

95.Project Xanadu, an attempt to ensure compensation to creators whenever even small chunks of intellectual property are used, was initiated in 1960. Xanadu FAQ, sec. 1b, June 29, 1996 <http://www.xanadu.com.au/xanadu/faq.html>.

96.*See Seybold Report on Desktop Publishing*, July 8, 1996 <http://www. media.sbexpos.com/OldHotStories/960702.htm> (describing digital object identifiers and the LicensIt product from NetRights).

97.*See* Stanford Copy Analysis Mechanism (SCAM)

<http://www-db.stanford.edu/~shiva/SCAM/scamInfo.html>; *see also* Hyperstamps CyberGumshoe Services <http://www.hyperstamps.com/misc/gumshoe.html> (offering a robotic search of the Internet for documents containing serialized document numbers that developers may insert (for a cost) into an HTML page); Intellectual Protocols' Copysight <http://www.ip2.com/copysight.cgi> (offering a service similar to Hyperstamps); *cf.* MarkWatch <http://www.markwatch.com/> (providing an automated monitoring service for trademark usage on the Internet); Alex Alben, *The Death of Copyright in a Digital World: The Reports are Slightly Exaggerated*, Ent. Law Rep., July 1995 (describing "bounty hunter" programs used by intellectual property owners to cut down on infringements; third-party attorneys bringing suits against infringers were allowed to keep any damages won in the actions).

98. *See* Digimarc <http://www.digimarc.com/~digimarc/>; Highwater FBI <http://www.highwaterfbi.com/>; SysCoP <http://syscop.igd.fhg.de/>; Argent, a product created by the Palo Alto startup Dice (reported in Ross, *supra* note 15, at 139). Tests have indicated that digital watermarks are resilient enough to survive most editing and are still discernible after numerous reproductions. Ben Long, *Watermarking Makes Impression on Photos*, MacWeek, Oct. 21, 1996, at 16, *available at* <http://www.macweek.com/mw_1040/ga_watermark.html>.

99. David Voss, *Stop That Copy*, Wired, Aug. 1994, at 34, *available at* <http://www.hotwired.com/wired/2.08/departments/electric.word.html>; *see also* Jim Warren, *GovAccess.107*, March 12, 1995 <http://www.eff.org/ftp/Publications/E-journals/GovAccess/govaccess.107> (describing a similar approach).

100. *See* Borsook, *Steal This Article*, *supra* note 41.

101. *See* Lance Rose, *The Copyright Escalator of Fear*, Boardwatch, Nov. 1994 at 92, (describing $500,000 settlement reached in Playboy v. Event Horizons BBS), *available at* <http://www.boardwatch.com/november/LEGALLY.htm>; Computer Industry Litig. Rep., Jan. 4, 1996 at 21634 (reporting on a $600,000 settlement reached in Sega of America v. The Ghetto); Playboy Enters. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993), *available at* <http://www.jmls.edu/cyber/cases/frena.txt>; Sega v. MAPHIA (N.D. Cal. Dec. 18, 1996) <http://www.bna.com/e-law/cases/sega2.html>; Sega v. Sabella, 1996 U.S. Dist. LEXIS 20470 (N.D. Cal. Dec. 18, 1996).

There have also been well-publicized criminal indictments, including actions against Davey Jones Locker, Rose, *supra* note 15, at 104, and Rusty & Edie's BBS, Michael A. Hobbs, *ACLU Cries Foul in Computer Raid*, The Plain Dealer, Feb. 19, 1993 at 3B.

102. *See, e.g.*, James Evans, *Internet Issue: Use of the Web Raises Copyright Concerns*, L.A. Daily J., Feb. 9, 1995, at 1.

103. If browsing the Web is an infringement because a copy of the page is made and sent to the user's computer, as proposed by the NII White Paper, *supra* note 2 at 64-65, then the linking site has arguably committed contributory infringement by substantially contributing to the user's infringement (which occurred during the process of browsing). *See* Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators*, 13 Cardozo Arts & Ent. L.J. 345, 353-56 (1995), *available at* <http://yu1.yu.edu:80/csl/journals/aelj/articles/13-2/elkin.html>. The assertion that browsing is an actionable infringement has met strong criticism. *See id.* at 354; Samuelson, *supra* note 3, at 137.

104. Although the term "implied license" is frequently bandied about on the Internet, the concept is rather amorphous under copyright law. At its heart, an implied license is an estoppel doctrine, arising because the infringing party detrimentally and justifiably relied on the intellectual property owner's actions.

105. *See* R. Lee Sullivan, *Toll Booths on the Info Highway*, Forbes, March 25, 1996, at 118.

106. *See* Maximized Software's SiteShield <http://www.maximized.com/products/siteshield/> (providing a product that prevents linking from all URLs other than those on the specific website); Kristi Coale, *Intellecast Smartens Up to Banner Bypass*, Wired News (Mar. 28, 1997) <http://www.wired.com/news/technology/story/2844.html> (describing how Intellicast, a weather site, prevented links to its weather maps which bypassed the associated banner advertisements).

107. This is one of the features of the Copysight service from Intellectual Protocols <http://www.ip2.com/copysight.cgi>.

108. For example, @home <http://www.home.net/> is deploying a network that permits users to use high-speed cable modems for Internet access. So that users will experience cable modem speeds as often as possible, @home will cache (or archive or mirror, depending on the terminology) the entire Internet on regional servers to which users will connect via their cable modems.

The recent start-up Marimba <http://www.marimba.com/> uses caching as a way to make the use of Java programs more robust.

Also, the number of offline browsers is growing. Offline browsers are software that automatically download some or all of an Internet site to the user's computer, allowing the user to browse without having to wait for the delivery of each page. *See, e.g.*, WebEx <http://www.gowebex.com/>, WebWhacker <http://www.ffg.com/whacker/index. html>, InContext Flashsite <http://www.incontext.com/products/flashsite/index.html> and DocuMagix HotCargo Express <http://www.documagix.com/products/hotcargo_express/welcome.html>.

109.*See* Lisa Sanger, *Caching on the Internet*, Spring 1996 <http://seamless.seamless.com/eric/cache.html>; Eric Schlachter, *Cache-22*, Intell. Prop. Mag. of the Recorder, Summer 1996, at 15, *available at* <http://www.ipmag.com/schlacht.html>.

110.Toys R Us v. Akkaoui, 1996 U.S. Dist. LEXIS 17090 (N.D. Cal. Oct. 29, 1996) (describing injunction granted in favor of a trademark owner against an infringing website requiring the website to notify all publishers of directories or lists to remove reference to the website and to flush all references to the website from their caches).

111.A different analysis might apply in regard to trade secret and trademark law. In the case of trade secrets, the owner must use efforts, whether technological or otherwise, to keep the information secret in order to preserve the information's status as a trade secret. In the case of trademarks, the owner must use quality control, whether technological or otherwise, to maintain the trademark.

112.*See, e.g.*, NII White Paper, *supra*, note 2, at 7-17.

113.At least two important exceptions to this general statement exist. First, the conclusion that loading a copy into RAM is an infringement creates a great deal of uncertainty for browsing. At a minimum, clarifying that browsing is not an actionable infringement would be helpful. Second, although generally a topic outside the scope of this paper, the conclusion reached in some cases that sysops are directly liable for copyright infringements occurring because users upload works subject to copyright onto their system has caused a great deal of consternation. If as a policy matter a consensus exists that sysops should not be liable in this circumstance, statutory clarification would be useful.

Reprinted with permission from The Berkeley Technology Law Journal

Cooley Alerts & Handbooks · Article Reprints · Press Releases · Search

Site Map · Disclaimer · Bookmark this Link · Frames Off
Copyright © 1994 - 1998 Cooley Godward LLP. All rights reserved.
COOLEY and COOLEY GODWARD are registered U.S. service marks of Cooley Godward LLP.

-CITE-

47 USC Sec. *230* 01/06/97

-EXPCITE-

TITLE 47 - TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS

CHAPTER 5 - WIRE OR RADIO COMMUNICATION

SUBCHAPTER II - COMMON CARRIERS

Part I - Common Carrier Regulation

-HEAD-

Sec. 230. Protection for private blocking and screening of offensive material

-STATUTE-

(a) Findings

The Congress finds the following:

(1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

(2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.

(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

(5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

(b) Policy

It is the policy of the United States -

(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

(c) Protection for ''Good Samaritan'' blocking and screening of offensive material

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of -

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

(FOOTNOTE 1)

(FOOTNOTE 1) So in original. Probably should be ''subparagraph

(A).''

(d) Effect on other laws

(1) No effect on criminal law

Nothing in this section shall be construed to impair the enforcement of section 223 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.

(2) No effect on intellectual property law

Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

(3) State law

Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

(4) No effect on communications privacy law

Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

(e) Definitions

As used in this section:

(1) Internet

The term ''Internet'' means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

(2) Interactive computer service

The term ''interactive computer service'' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) Information content provider

The term ''information content provider'' means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

(4) Access software provider

The term ''access software provider'' means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

(A) filter, screen, allow, or disallow content;

(B) pick, choose, analyze, or digest content; or

(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

-SOURCE-

(June 19, 1934, ch. 652, title II, Sec. 230, as added Feb. 8, 1996, Pub. L. 104-104, title V, Sec. 509, 110 Stat. 137.)

-REFTEXT-

REFERENCES IN TEXT

The Electronic Communications Privacy Act of 1986, referred to in subsec. (d)(4), is Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, as amended. For complete classification of this Act to the Code, see Short Title of 1986 Amendment note set out under section 2510 of Title 18, Crimes and Criminal Procedure, and Tables.

-COD-

CODIFICATION

Section 509 of Pub. L. 104-104, which directed amendment of title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.) by adding section 230 at end, was executed by adding the section at end of part I of title II of the Act to reflect the probable intent of Congress and amendments by sections 101(a), (b), and 151(a) of Pub. L. 104-104 designating Sec. 201 to 229 as part I and adding parts II (Sec. 251 et seq.) and III (Sec. 271 et seq.) to title II of the Act.

-SECREF-

SECTION REFERRED TO IN OTHER SECTIONS

Cooley Godward LLP

Cooley Alert

October 1998

Website Provider Liability for User Content and Actions

Many websites have found that developing an online "community" is crucial to obtaining their business objectives. As a result, user-generated content is ubiquitous online.

While user-generated content can facilitate a website's objectives, it raises a host of thorny legal issues. Default legal rules may impose liability on websites for intellectual property infringement and other harms caused by their users, and a single bad user could cause liability ranging into the millions of dollars. There have now been over a dozen cases on the topic, some with sensible rulings and others raising the specter of, effectively, unlimited liability.

Websites planning to permit users to exchange content should implement a number of techniques to manage their potential risk. This Cooley Alert identifies some of the problems arising from permitting user-generated content on your website and then provides a few general suggestions for managing the associated risks.

Sources of Liability

Below are a few of the most common legal issues websites encounter when permitting user-generated content.

Intellectual Property Infringement

Copyright: Copyright law recognizes three types of liability: direct, contributory, and vicarious.

Direct infringement occurs when an infringer copies a copyrighted work. Direct liability is a strict liability offense, and thus does not require the infringer to know of the infringement. If direct infringement applies, a website provider would be liable if a user posts a copyrighted work that is subsequently downloaded or viewed by others. While some courts have held service providers directly liable for user-committed copyright infringement, other courts have rejected imposing direct liability as unduly harsh and instead analyze infringement claims against website providers under contributory or vicarious liability.

Contributory infringement occurs when a party knows of an infringing activity and substantially participates in that activity. While the existing cases have not definitively addressed when a website is contributorily infringing based on its users' activities, the cases generally have suggested a notice-based liability standard. In other words, once a website receives notice that a user is committing infringement, the website will be deemed to be substantially participating in the infringement if it does not remove the infringement within a reasonable period of time. (Note: The courts have not yet defined what is a suitable "notice" that alleges copyright infringement; for now, each notice must be analyzed on its own terms.) Of course, if a website actually knows of a particular infringement based on its practices, this knowledge will also trigger the duty to act. Thus, to minimize exposure for contributory copyright infringement, websites should (a) try to reduce actual knowledge of user-generated content by not monitoring their services, and (b) respond promptly to notices alleging that a user is committing copyright infringement.

Vicarious copyright infringement occurs when a party has the right and ability to control the infringer and reaps a direct financial benefit from the infringing activity. As a practical matter, many websites take the position that they have little or no ability to control their users. However, cases suggest that even nominal indicia of the right and ability to control users—such as a user agreement that contains subjective and arbitrary restrictions on users, or a pattern of disabling users' accounts or yanking user content—could, when aggregated, lead to a finding that the website has the "right and ability to control" the infringing user.

Some cases have found "direct financial benefit" merely when parties charge flat fees for their services, even if these fees do not vary based on the amount of infringement committed by others. However, if these precedents are not followed, it is likely that a website will be deemed to have a direct financial benefit if its business model creates additional revenues as increased infringement occurs. This may occur when a website charges a transaction fee based on user activity (which includes situations where user activity is infringing) or when a website delivers advertisements on user content (which includes infringing content). In these circumstances, it is imperative that the website reduce all indicia of their right and ability to control their users—or else, regardless of their claim that it was not practical or possible to manage their users, the

website may become vulnerable to claims, no matter how unjustified they may seem, for act of infringement committed by users.

This summer, both the House of Representatives and the Senate passed versions of the Digital Millennium Copyright Act (the "DMCA"). It is expected that differences between the versions of the bill will be resolved in the joint House/Senate committee and the final bill will be enacted. The DMCA does contain a number of provisions purporting to limit website liability for user-committed copyright infringements, but as currently written, the DMCA does not meaningfully limit potential contributory or vicarious liability on the part of websites. Thus, as a practical matter, the DMCA is not expected to affect the current state of the law with respect to possible website liability for contributory or vicarious copyright infringements.

Trademark: Trademark law prevents the use of trademarks of others in a manner that creates a likelihood of confusion about the source of goods or services or in a manner that dilutes the value of the trademark. As with copyright law, liability can be found for direct, contributory, or vicarious infringement.

Of these three types of liability, websites face the greatest risk that they may be contributorily infringing based on their users' content. Contributory trademark infringement occurs when a party supplies a "product" (such as a web page) knowing that the "product" is being used to infringe a third party's trademark. Thus, in this respect, contributory trademark infringement appears to have the same characteristics as contributory copyright infringement—actual knowledge or notice of infringement initiates a duty to cease further infringement or face liability.

Defamation and Other "Publisher/Speaker" Torts

Section 230(c)(1) of the Communications Decency Act, passed in 1996, says "no provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider." To date, courts have treated this language as a nearly complete bar against liability for users' defamatory postings.

While this statutory safe harbor has provided some welcome relief to websites, it is not a panacea. First, the safe harbor applies only to information "provided by another information content provider." Thus, information provided by employees and, perhaps, some independent contractors may still create liability. Second, the only claims courts have determined to be covered by the statute are defamation and certain conduct related to child pornography, and it is unclear whether other claims such as publicity or privacy rights violations would be covered by the statute. Intellectual property and federal obscenity/child pornography claims are not affected by the statute, and the words "publisher or speaker" have not been sufficiently interpreted to explain what other types of claims will be protected under the statute. Finally, the safe harbor applies only to "interactive computer services," a term which is not well-defined in the statute and which may not cover websites.

Obscenity and Child Pornography

No cases specifically address website liability for user-generated obscenity or child pornography. Websites faced with state law obscenity or child pornography charges can argue that such claims qualify for immunity under §230(c), but this defense is not certain. Further, the safe harbor in the Communications Decency Act (discussed above) expressly excludes federal criminal obscenity and child pornography laws from its safe harbor. Thus, websites could be liable for user-generated obscenity or child pornography in certain circumstances.

Other Claims

Until the scope of the safe harbor in the Communications Decency Act is more fully understood, the range of potential claims against websites is impossible to define. If the safe harbor defense is not available, websites will need to develop other defenses, if they can, against claims for user-caused harms and attendent claims that the website knew of the harm and failed to take reasonable actions to prevent or remedy the harm.

Suggestions For Risk Management

In light of the above analysis, Cooley Godward continues to believe that websites should take steps to avoid knowing their users' activities and content and, in most cases, reduce indicia of their right and ability to control user behavior and content. Thus, we propose that websites consider the following recommendations:

1. Do Not Actively Monitor the Website. Active monitoring of the website will give the website actual or putative knowledge of user conduct and content. Thus, active monitoring creates the possibility that a website will be liable for all user-caused harms except those preempted by the safe harbor in the Communications Decency Act.

2. Consider Empowering Independent Contractors to Monitor your Site. Some websites believe that active

monitoring is crucial to their business objectives. In these cases, the websites should have independent contractors do the monitoring. If done properly, the website will not be liable for the independent contractors' monitoring or knowledge of user content. However, to ensure that the independent contractors will not be deemed agents of the website—in which case this risk management strategy will have failed—the independent contractors must be given the authority necessary to resolve problems they find.

3. Respond to Complaints. Although in general websites should minimize contact with user-generated content, if a website receives a legitimate complaint about user content, it usually has a duty to respond promptly (unless the claim is preempted by the safe harbor in the Communications Decency Act).

4. Review the User Agreement. Provisions enabling websites to blacklist subscribers or edit content based on subjective or arbitrary standards provide strong evidence of the site's right and ability to control its users and their content. Thus, user agreements should only prohibit users from engaging in conduct that is illegal or tortious, or that interferes with the technological operation of the site.

5. Train Employees. All employees who interact with the website can take legally significant actions that could undermine a risk management strategy. Thus, the website's risk management strategy should be explained to all employees, and employees responsible for dealing with website problems should be given special training on how to implement the strategy.

6. Insurance. Insurance is becoming increasingly available for risks associated with user-generated content. Insurance provides an excellent way to convert the risk of major liability into a manageable expense.

Conclusion

Deploying an effective strategy to manage risks associated with user-generated content is a complex and multifaceted effort with significant implications for the website, its relations with its users, and its associated liability. This Cooley Alert provides only a overview of the problems. Each website has its own unique business and technical practices that can minimize—or exacerbate—the problems described herein. To get our help in the process of developing and implementing a risk management strategy, contact one of the members of our Information Technology group.

Contact Information

Palo Alto, CA

Diane Savage 650-843-5077
savagedw@cooley.com

San Francisco, CA

Paul Startz 415-693-2048
startzp@cooley.com

San Diego, CA

Bradford Biddle 619-550-6301
biddlecb@cooley.com

Boulder, CO

Steve Dupont 303-546-4017
dupontsn@cooley.com

Kirkland, WA

Chris Wright 425-893-7800
wrightcw@cooley.com

Copyright © 1994 - 1998 Cooley Godward LLP. All rights reserved.
COOLEY and COOLEY GODWARD are registered U.S. service marks of Cooley Godward LLP.

[Page 1]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

PLAYBOY ENTERPRISES, INC.,
Plaintiff,

v.

RUSS HARDENBURGH, INC.,
Defendant.

No. 1:93 CV 0546.
Filed Nov. 25, 1997.

SAM H. BELL, District Judge.

ORDER:

This case raises the question of a computer bulletin board system operator's liability for copyright and trademark infringement regarding information available to its customers through their home computers. Plaintiff Playboy Enterprises, Inc. ("PEI") asks the court to find that Defendants Rusty-N-Edie's, Inc. ("RNB") and Russ Hardenburgh are liable for direct and/or contributory copyright infringement with respect to 412 graphic image files ("GIFs") which were allegedly available to paying customers of Defendants' bulletin board service (the "BBS"). These files, asserts PEI, contain illegal copies of adult photographs from PEI's Playboy Magazine. PEI also claims that Defendants' violated section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a), by removing the name or trademark of PEI and distributing the photographs under other names for a profit. Defendants answer that there are genuine issues of material fact with respect to each of Plaintiff's claims, precluding summary judgment.

[Page 2]

The court has considered the evidence and arguments of the parties, and is now prepared to offer its decision in this matter.

Plaintiff's motion for summary judgment is granted with respect to its claims of direct and contributory copyright infringement against both RNE and Mr. Hardenburgh. Plaintiff's motion is denied with respect to its Lanham Act claim, which claim shall be set forth for trial.

The court's reasoning in this matter is set forth below.

Background

A computer bulletin board service ("BBS") offers home computer owners a method for obtaining information from a central source by use of a modem.[1] Remote computers access the central service through telephone lines. Files of information are stored in the central system, and subscribers may either "download" information into their home units, or "upload" information from their home units into the central files. The owner of the service controls the terms by which remote computer owners will be able to access the system, and typically will control the conditions under which information may be downloaded or uploaded.

BBS owners often provide other services to subscribers, including electronic mail capabilities, "chat

rooms" where many subscribers may communicate at once, and Internet access to the World Wide Web. Local bulletin board services such as the one in this case might be

[Page 3]

distinguished from massive on-line services such as America On-Line or Compuserve, which provide similar services to customers on a much larger scale.

Defendant RNE and its President, Russ Hardenburgh, began operating a local BBS out of Boardman, Ohio in the early days (relatively speaking) of this technology. In July of 1988, "Rusty-N-Edie's BBS" became available to owners of home computers. (2nd Hardenburgh Aff. Para. 1.) For a fee, subscribers received access to certain files which were otherwise off limits to the general public, and had the right to download a set number of megabytes of electronic information from these files every week. (Hardenburgh dep. pp. 120-122.) The BBS also provided e-mail services, chat lines, advertisements for goods, computer technical assistance, and a "matchmaker" dating service. (2nd Hardenburgh Aff. Para. 3.)

By January of 1993, the central BBS had grown to 124 computers, with nearly 6000 subscribers. (2nd Hardenburgh Aff. Para. 6.) Approximately 105,000 to 110,000 files were available for downloading, nearly half of which were graphic image files, or "GIFs." (*Id.*) A GIF is created by scanning a photograph to create digital data that can be run through a computer. GIFs from Rusty-N-Edie's BBS could be downloaded by the customer to his or her home computer, and could be viewed only with the assistance of certain specialized software. (*Id.*) Approximately 40,000 of the GIFs available to subscribers at this time, Defendants admit, contained "adult" photographs. (1st Hardenburgh Aff. Para. 6.)

To increase its stockpile of available information, and thereby its attractiveness to new customers, Defendants provided an incentive to encourage subscribers to upload information onto the BBS. Subscribers were given a "credit" for each megabyte of electronic data that they uploaded onto the system. For each credit, the subscriber was entitled to download 1.5 extra

[Page 4]

megabytes of electronic information, in addition to the megabytes available under the normal terms of subscription. (Hardenburgh dep. p. 157.) According to Defendants, information uploaded onto the BBS went directly to an "upload file" where an RNE employee briefly checked the new files to ascertain whether they were "acceptable," meaning, not pornographic, and not blatantly protected by copyright. (Hardenburgh dep. p. 138-142.)

PEI is understandably concerned that on-line systems can be used to transmit copies of its copyrighted photographs to people who have not themselves purchased Playboy Magazine. In the early 1990s, PEI employee Anne Steinfeldt was given the job of scanning on-line systems to determine whether such photographs were available to subscribers via their home computers. (2nd Steinfeldt Aff. Para. 1.) In November of 1992, Ms. Steinfeldt subscribed to Rusty-N-Edie's BBS under the pseudonym "Bob Campbell." (*Id.* at Para. 2.) She conducted key word searches in the files available on the BBS, and claims to have downloaded approximately 100 GIFs from the BBS which contained reproductions of PEI's photographs. (*Id.* at Para. 5.) She transferred these files to floppy disks, and then delivered the disks to PEI photo-librarian Timothy Hawkins. (Hawkins Aff. Para.Para. 2, 3.) Mr. Hawkins states that he examined the files by displaying the images on his computer monitor and comparing those images with photographs from Playboy Magazine. (*Id.* at Para.Para. 3, 4.)

On March 11, 1993, PEI filed its original complaint against RNE and Mr. Hardenburgh in this court, alleging copyright and trademark infringement. (Docket # 1.) The case was assigned to District Judge Battisti. On January 7, 1994, PEI moved for summary judgment on its claims of copyright infringement with respect to 99 GIFs allegedly downloaded from the BBS by Ms. Steinfeldt and reviewed by Mr. Hawkins. (Docket # 28.) PEI listed the

[Page 5]

titles of the 99 GIFs at issue in its Exhibit A but only submitted ten actual copies of the allegedly infringing images. (Docket # 29.) PEI paired these ten reproductions of computer screens with ten virtually identical photographs from Playboy Magazine. (*Id.*) PEI also produced the certificates of copyright for each of the PEI photographs listed in its Exhibit A. (*Id.*) Based upon these submissions and the accompanying affidavits of its employees, PEI argued that Defendants could raise no genuine issue of material fact to dispute the assertion that all 99 GIFs had appeared on the BBS. (*Id.*) Defendants, PEI argued, were jointly and severally liable for copyright infringement as a matter of law.

On January 31, 1994, PEI moved for summary judgment on its Lanham Act unfair competition claim. (Docket # 33.) PEI argued that Defendants had falsely implied that they were the source of PEI's images by adding text to PEI photographs that was not present originally, and by deleting text that was originally present. (*Id.*) PEI claimed that the words "Rusty-N-Edies" had been added to some of the photographs, along with the telephone number for one of Defendants' BBS phone lines. (Docket # 34.) PEI provided one actual example of this activity. (*Id.*)

Defendants responded to PEI's motions for summary judgment on February 24, 1994, arguing that there were genuine issues of material fact with respect to each of PEI's claims. (Docket # 40.) Defendants argued that PEI's submissions did not prove that the 99 GIFs listed in Exhibit A were actually present on the BBS. (*Id.*) Mr. Hardenburgh claimed that he had reviewed the floppy disks in question, and had found them to contain 85 GIFs, not 99. Only 82 of the files on the disks, he asserts, were even listed in Plaintiff's Exhibit A, four of which were created or modified after Ms. Steinfeldt turned the disks over to Mr. Hawkins. (1st Hardenburgh

[Page 6]

Aff. Para. 5.) Defendants argued that these inconsistencies cast doubt on the credibility of PEI employees Steinfeldt and Hawkins, and precluded summary judgment in PEI's favor. (Docket # 40.)

PEI replied to Defendants on June 10, 1994, and in doing so brought new evidence to light. (Docket # 46.) PEI explained to the court that on January 30, 1993 the Federal Bureau of Investigation had conducted an unrelated search of the Hardenburgh premises pursuant to a search warrant, and had seized Defendants' BBS equipment. (*Id.*; 1st Hardenburgh Aff. Para. 2.) In connection with this search, the FBI had created computer tapes (the "FBI Tapes") which contained all of the information present on the BBS at that time, including all GIFs available to subscribers for downloading. (1st Tesnakis Aff.) Both sides of the litigation, PEI explained, were in possession of copies of these tapes. (Gibson Aff. Para.Para. 4, 5, 6.) Having reviewed the tapes, PEI withdrew its motion for summary judgment with respect to 79 of the 99 GIFs originally at issue. PEI was apparently unable to confirm that these 79 GIFs were on the BBS at the time of the FBI search. (Docket # 46.) With respect to the other 20 GIFs, however, PEI asserted that the FBI Tapes conclusively established that these files were present on Defendants' BBS on January 30, 1993, and that they directly infringed PEI's copyrights. (*Id.*) PEI submitted copies of these 20 GIFs as extracted from the FBI Tapes, and also submitted the corresponding 20 photographs from Playboy Magazine. (Exhibit 2 to Tesnakis Aff.) PEI noted that it would continue to study the FBI Tapes to determine whether a future motion for summary judgment could be filed with respect to other files present on the BBS which may have infringed PEI's copyrights. (Docket # 46.)

Defendants surreplied to Plaintiff's answer on July 11, 1994. (Docket # 51.)

[Page 7]

Defendants implied that any PEI photographs which appeared on the BBS were placed there by RNE *subscribers,* not RNE employees. (*Id.*) Because Defendants had not themselves taken part in any infringing activity, they asserted, they could not have directly infringed PEI's copyrights. (*Id.*)

On September 14, 1994, Magistrate Judge Bartunek issued a Report and Recommendation regarding PEI's motions for summary judgment. (Docket # 60.) The Magistrate recommended that the court grant

Plaintiff's motion for summary judgment regarding Defendants' liability for direct copyright infringement. (*Id.*) The Magistrate found that there was no dispute that PEI owned the copyrights in question and that the 20 GIFs at issue had, in fact, appeared on Defendants' BBS. (*Id.*) Also, it was abundantly clear to the Magistrate that the GIFs produced by Plaintiff were copies of the 20 PEI photographs submitted into evidence. (*Id.*) As to Defendants' claim that it was BBS *subscribers* who uploaded the information onto the system, the Magistrate felt that this argument was immaterial in relation to a finding of copyright infringement. (*Id.*)

With respect to any Lanham Act violations, alternatively, the Magistrate recommended that the court deny Plaintiff's motion. (*Id.*) The Magistrate felt that in order to prevail on their Lanham Act claim, PEI would have to prove that it was Defendants, and not their subscribers, who engaged in activity which misled consumers about the source of the images. (*Id.*)

Both Plaintiff and Defendant filed objections to the Magistrate's Report and Recommendation. (Docket #s 64, 66, 69.)

On November 1, 1994, following Judge Battisti's death, the case was transferred

[Page 8]

to Senior Circuit Judge Krupansky. (Docket # 71.) Soon thereafter, on January 17, 1995, PEI filed its third motion for summary judgment. (Docket # 74.) As promised, PEI had scrutinized the FBI Tapes and announced that it was now prepared to prove that 392 additional GIFs containing copies of PEI photographs were present on Defendants' BBS at the time of the FBI search. (Docket # 75.) PEI produced, for the court's consideration, copies of each and every one of the GIFs at issue, in addition to the corresponding PEI photograph. (Exhibit D to 2nd Tesnakis Aff.) PEI also produced certificates of copyright for each photograph. (Exhibit B to 2nd Tesnakis Aff.) PEI repeated their claim that Defendants were liable for direct copyright infringement, but argued in addition that Defendants were liable for contributory copyright infringement. (Docket # 75.) PEI produced the deposition testimony of three RNE employees, each of whom stated that any GIFs which were uploaded onto the BBS were placed in an upload file, and were not released onto the system for subscribers until they were reviewed by RNE staff. (Hardenburgh dep., Little dep., McFarland dep.) Defendants responded, echoing many of the arguments they had made previously. (Docket # 88.) Defendants also argued that a finding of copyright infringement on the part of a computer bulletin board service would "halt the computer age at its inception" by overburdening BBS owners with the "impossible" task of screening their systems for any and all copyrighted material. (*Id.*) On March 1, 1996 the case was transferred here. (Docket # 104.)

The parties have offered numerous submissions and arguments in addition to those described above, some of which will be touched upon below. The question presented in this litigation, however, has remained fundamentally the same throughout. It is: *has PEI produced sufficient evidence to warrant summary judgment on its claims of copyright and trademark infringement?*

[Page 9]

Standard of Review

The Court of Appeals for the Sixth Circuit recently summarized the standard of review governing motions for summary judgment under > Federal Rule of Civil Procedure 56:

> Summary judgment is appropriate where 'there is no genuine issue of material fact ... and the moving party is entitled to judgment as a matter of law.'.... [The] court must view all facts and inferences drawn therefrom in the light most favorable to the non-moving party.
>
> The moving party has the burden of conclusively showing that no genuine issue of material fact exists. Nevertheless, in the face of a summary judgment motion, the nonmoving party cannot rest on its pleadings but must come forward with some probative evidence to support its claim.

'By its very terms, this standard provides that the existence of some alleged factual dispute between the parties will not defeat an otherwise properly supported motion for summary judgment; the requirement is that there be no genuine issue of material fact.' The dispute must be genuine and the facts must be such that if they were proven at trial, a reasonable jury could return a verdict in favor of the nonmoving party. If the disputed evidence 'is merely colorable or is not significantly probative, summary judgment may be granted.'

Leo LaPointe v. United Autoworkers Local 600, 8 F.3d 376, 378 (6th Cir.1993) (citations omitted). With this standard in mind, the court shall analyze the PEI's motions for summary judgment.

Law and Analysis

PEI has moved for summary judgment on three independent claims. Each claim, the court will assume, applies to the 412 GIFs submitted into evidence.

I.

Direct Copyright Infringement

To sustain a case of direct copyright infringement, Plaintiff must first satisfy two

[Page 10]

threshold requirements. Plaintiff must prove "(1) ownership of a valid copyright, and (2) copying [by the defendants] of constituent elements of the work that are original." *Feist Publications, Inc. v. Rural Tel. Serv. Co.,* 499 U.S. 340, 361, 111 S.Ct. 1282, 1296, 113 L.Ed.2d 358 (1991); *Hi-Tech Video Prods., Inc. v. Capital Cities/ABC, Inc.,* 58 F.3d 1093, 1095 (6th Cir.1995); *Wickham v. Knoxville Int'l Energy Exposition, Inc.,* 739 F.2d 1094, 1097 (6th Cir.1984). PEI's certificates of copyright create a presumption of the validity of the copyrights in this case. 17 U.S.C.A. Section 410(c). Although the presumption may be rebutted, it is the burden of the party challenging the copyright to do so. *Gates Rubber Co. v. Bando Chem. Indus., Ltd.,* 9 F.3d 823, 831 (10th Cir.1993). Defendants have not rebutted the ownership or validity of PEI's copyrights, which the court takes as established.

To prove the "copying" element, Plaintiff may either produce direct evidence that Defendants copied their material, or may create an inference that copying occurred by showing: (1) that Defendants had access to the protected work, and (2) that the two works are substantially similar. *Wickham,* 739 F.2d at 1097; *Novelty Textile Mills, Inc. v. Joan Fabrics Corp.,* 558 F.2d 1090, 1092 (2d Cir.1977). Plaintiffs have no difficulty establishing the "copying" element. First, Defendants clearly had access to Playboy Magazine and the photographs contained therein at the time that the GIFs allegedly appeared on their BBS. Playboy Magazine is publicly available material. Second, there is no arguing that the 412 GIFs produced by PEI are not substantially similar to the 412 PEI photographs in evidence. They are virtually exact reproductions.

Having satisfied these threshold requirements, Plaintiff can establish direct infringement by proving that Defendant used the accused copies in any of the ways described in > Section 106 of the Copyright Statute. Under 17 U.S.C. Section 106, a copyright owner has the

[Page 11]

exclusive right to, among other things: (a) reproduce the copyrighted work, (b) distribute copies of the copyrighted work to the public by sale or other transfer of ownership, and (c) display the copyrighted work publicly.

A.

Findings of Fact

This court is bound to construe all of the evidence in a light most favorable to Defendants, the non-moving parties. In so doing, the court finds that Plaintiff has conclusively shown the following to be true: (1) in January of 1993, Defendants were operating a computer BBS; (2) prior to this date, Defendants adopted an incentive program to encourage their subscribers to upload information onto the BBS in order to increase the stockpile of information available to customers (Hardenburgh dep. p. 157); (3) information uploaded onto the system from subscribers' home computers was held in an upload file where it was briefly screened by RNE employees before it was released, by those employees, onto the general BBS; (Hardenburgh dep. p. 138-142); (4) Defendants had notice that PEI was in the habit of enforcing its copyrights against BBS owners (Hardenburgh dep. p. 192, Hardenburgh Aff. Para. 5); (5) as of January 30, 1993, when the FBI Tapes were created, 412 GIFs were available on Defendants' general BBS which contained virtually exact reproductions of copyrighted photographs from Playboy Magazine. (Exhibit 2 to 1st Tesnakis Aff., Exhibit D to 2nd Tesnakis Aff.)

B.

Defendants' Arguments

According to Defendants, the facts described above are insufficient to warrant a judgment of direct copyright infringement. First, they argue that they did not in any way usurp

[Page 12]

one of the protected rights of PEI as a copyright owner. Defendants claim that they did not "reproduce" copies of PEI photographs by simply providing an incentive to subscribers to upload electronic data onto the BBS. It was the subscribers who scanned the copyrighted photographs and turned them into electronic data, and it was subscribers who uploaded the information onto the system. Similarly, they claim that they never "distributed" PEI photographs to their customers because it was the customers *themselves* who chose whether or not to download the GIFs from the central system to their home computer. Defendants describe themselves as passive providers of the space in which the pictures were passed from one party to another. Defendants argue that they never "publicly displayed" PEI photographs either, because subscribers to the BBS could only view the GIFs on their own computers in the privacy of their own home, and only with the help of certain specialized software.

Defendants make a number of policy arguments as well. They point out that BBS operators must develop methods of obtaining new information in order to stay competitive in the crowded on-line computer market. New customers will be drawn to the BBS or on-line service which provides the most information. The incentive system developed by RNE was a reasonable way, then, to maintain competitiveness and allow the company to grow. At the same time, they argue that it would have been impossible to police each and every uploaded file to ensure that it did not contain copyrighted material. While RNE employees could quickly view an uploaded file to determine whether it contained clearly inappropriate material such as, for instance, child pornography, it would be unthinkable to require these employees to determine the *source* of each and every photograph to ensure that there was no possibility of copyright infringement. To place such liability on the owners of a BBS, Defendants argue, is an excessive burden on the rights of

[Page 13]

free speech as embodied in the First Amendment.[2] In addition, they claim that such liability threatens to dismantle the computer on-line industry.

Even if, Defendants continue, the on-line industry as a whole is not destroyed by imposing copyright liability on service providers, such liability will irreversibly disadvantage local BBS owners in relation to massive on-line systems. Local BBS operators are less able to spread the cost of copyright liability to their more limited pool of subscribers. The outcome of a regime which imposes direct liability on owners of on-line systems, they warn, is the eventual extinction of local providers. Defendants claim that such an outcome could not be consistent with the primary objective of copyright law, which is "not to

reward the labor of authors, but '[t]o promote the progress of Science and useful Arts.'" *Feist,* 499 U.S. at 349.

good ergo !!

C.

Plaintiff's Arguments

Plaintiff, on the other hand, argues that copyright laws are meant to protect copyright owners from a situation in which their private material is used, without permission, by a non-owner for profit. Defendants, PEI claims, profited from a system in which PEI photographs were illegally provided to consumers who did not themselves purchase Playboy Magazine. Instead, these consumers purchased subscriptions to Rusty-N-Edie's BBS, and received the Playboy pictures for free.

Plaintiff notes that Defendants were aware that PEI was in the habit of enforcing its copyrights. Defendants should have, therefore, used their screening procedures to keep any

[Page 14]

and all PEI photographs off of the BBS. Instead, PEI asserts, Defendants adopted a policy of willful blindness, ignoring the strong likelihood that PEI pictures were being copied and sent onto the system, yet encouraging subscribers to continue to upload any and all photographs. Procedurally, RNE employees viewed each and every photograph that was uploaded onto the system, and then moved those photographs that were not discarded from the upload file to the central files where they became available to RNE customers. If direct copyright infringement carries with it a volitional element, Plaintiff argues, that requirement is satisfied by the participation of the RNE employees in the screening process.

In response to Defendants' policy arguments, Plaintiff admits that it may have been costly for Defendants to police their system to prevent copyrighted information from passing through it. Plaintiff asserts that it is more reasonable, however, to place the cost of protecting against copyright infringement on the parties who provide the system which facilitates infringement, rather than the innocent owner of the copyright. Even if this type of liability regime favors larger on-line providers, Plaintiff argues that the diversity of the on-line computer industry is not the responsibility of copyright owners. If Defendants cannot divine an efficient way to operate a computer BBS free of copyrighted material, Plaintiff argues, then Defendants have the option of leaving the industry.

Plaintiff also points out, correctly, that a finding of direct copyright infringement carries no scienter requirement. PEI need not show that Defendants had any knowledge that PEI materials were available to their subscribers. PEI need only establish the threshold elements, ownership and copying, and that Defendants violated an exclusive right of a copyright owner.

According to Plaintiff, the mere fact that Defendants provided the space in which

[Page 15]

PEI photographs were copied and exchanged is sufficient to warrant a finding of direct copyright infringement. In the event that the court finds there is a further volitional requirement, PEI points to the screening procedures and the participation of RNE employees in moving PEI photographs onto the system. These facts, Plaintiff argues, establish Defendants' direct participation in the infringement which took place.

C. [D.]

Case Law

The case law in this area is relatively sparse, and the matter is one of first impression in our circuit. The court offers a brief discussion of the major cases in the area, to provide a foundation for its decision today.

especially when the court does incomplete analysis!

In *Playboy Enterprises v. Frena,* 839 F.Supp. 1552 (M.D.Fla.1993), District Judge Schlesinger was presented with facts not unlike those which are presently before this court. PEI had sued the owner of a BBS for direct and contributory copyright infringement because copies of its photographs were available to BBS subscribers. *Id.* at 1554. The defendant BBS owner argued that it was his subscribers, and not he, who had placed the photographs on the system. *Id.*

The differences between *Frena* and this case are few, but should be mentioned. First, in the *Frena* case, the defendant admitted that the photographs appeared on his BBS. There has been no such concession here, though Defendant has made no factual showing to the contrary. Second, and more importantly, there is no discussion in the *Frena* case of any screening procedure utilized by the defendant's BBS before uploads were released onto the

[Page 16]

general system. It appears that subscribers to Mr. Frena's BBS were able to upload information directly into the central files where they became immediately available to other subscribers. Mr. Frena, then, was even more of a passive participant in the copying and exchange of copyrighted photographs than are the Defendants in this case.

District Judge Schlesinger held that Mr. Frena was liable for direct copyright infringement. *Id.* at 1556-57. As in our case, PEI easily established the threshold elements of ownership/validity and copying. Moving on to the more difficult consideration, the court found that defendant had violated PEI's exclusive "distribution" and "display" rights. *Id.*

The court found that defendant had "distributed" PEI photographs simply by providing the space in which those photographs were uploaded and downloaded. The court stated that, "[t]here is no dispute that Defendant Frena supplied a product [the BBS] containing unauthorized copies of a copyrighted work. It does not matter that Defendant Frena claims he did not make the copies itself [sic]." *Id.* at 1556. Judge Schlesinger apparently felt that a finding of direct copyright infringement does not carry with it a volitional element, or, if it does, that such requirement was satisfied by defendant's past action of setting up the BBS.

In regard to the violation of PEI's "display" rights, the court defined the word broadly, to include:

> the projection of an image on a screen or other surface by any method, the transmission of an image by electronic or other means, and the showing of an image on a cathode ray tube, or similar viewing apparatus connected with any sort of information storage and retrieval system.

Id. (citing H.R.Rep. No. 1476, 94th Cong., 2d Sess. 64 (Sept. 3., 1976), reprinted in U.S.Code Cong. & Admin. News 1976 p. 5659, 5677). The fact that PEI materials were only available to BBS subscribers did not change the public nature of the "display." *Id.* (citations omitted). The court

[Page 17]

did not consider whether Mr. Frena was liable for contributory copyright infringement.

In *Sega Enterprises Ltd. v. Maphia,* 857 F.Supp. 679 (N.D.Cal.1994), a computer software company sued the owner of a BBS for copyright infringement because copyrighted video games were available to BBS subscribers. The court granted plaintiff's request for a preliminary injunction, finding that plaintiff had shown a likelihood of success on the merits with respect to its claims of direct and contributory copyright infringement. *Id.* at 686. Plaintiff had shown its ownership of valid copyrights, and had proven that its games were available on defendant's system. *Id.*

The court was explicit in its discussion of contributory copyright infringement, holding that defendant's knowledge and encouragement of the infringing activity was sufficient to establish contributory liability.

→ !! Sega ct reversed Hotly in 1996 !!

Id. at 687. The court was less clear on the specific factors that led it to its finding of direct infringement. The court stated:

> Sega has established a *prima facie* case of direct copyright infringement under 17 U.S.C. § 501. Sega has established that unauthorized copies of its games are made when such games are uploaded to the MAPHIA bulletin board, here with the knowledge of Defendant Scherman. These copied games are thereby placed on the storage media of the electronic bulletin board by unknown users.
>
> Sega has established that unauthorized copies of these games are also made when they are downloaded to make additional copies by users, which copying is facilitated and encouraged by the MAPHIA bulletin board.

Id. at 686 (citations omitted). Because knowledge is not an element of direct infringement, the court seems to be saying, as in *Frena,* that the mere creation of a BBS is sufficient to establish direct infringement liability where copyrighted material appears on the system.

In *Religious Tech. Center v. Netcom On-Line Comm.,* 907 F.Supp. 1361

[Page 18]

(N.D.Cal.1995), District Judge Whyte departed from the reasoning of *Frena* and *Sega.* The owner of certain copyrighted religious material sued a BBS operator when the material was unlawfully copied and criticized on his BBS. The court in *Netcom,* however, refused to hold the BBS liable for direct infringement based simply on the creation of a space where infringing activity occurred. The court reasoned:

> Netcom's act of designing or implementing a system that automatically and uniformly creates temporary copies of all data sent through it is not unlike that of the owner of a copying machine who lets the public make copies with it. Although some of the people using the machine may directly infringe copyrights, courts analyze the machine under the rubric of contributory infringement, not direct infringement.

Id. at 1369. To impose direct infringement liability on a BBS where the operator did nothing more than provide space where information is exchanged, "would result in liability for every single ... server in the worldwide link of computers transmitting [subscriber's] message to every other computer." *Id.* Although the copyright statute creates a strict liability regime, the court noted that "there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party." *Id.*

D. [E.]

Defendants' Liability for Direct Copyright Infringement

As a legal matter, the court would agree with Judge Whyte that a finding of direct copyright infringement requires some element of direct action or participation, for two primary reasons. First, the statute is cast in terms of activities which are reserved to copyright owners. 17 U.S.C. § 106. It follows that an infringer must actually engage in one of those

[Page 19]

activities in order to directly violate the statute. Setting up a computer bulletin board is not one of those activities. Merely encouraging or facilitating those activities is not proscribed by the statute. Second, it is the area of contributory liability which allows "the imposition of liability on certain parties who have not themselves engaged in the infringing activity." *Sony Corp. v. Universal Studios, Inc.,* 464 U.S. 417, 435, 104 S.Ct. 774, 785, 78 L.Ed.2d 574 (1984) (footnote omitted). There would be no reason to bifurcate copyright liability into the separate categories of direct and contributory if any remote causal connection

to copyright infringement could be analyzed under theories of direct infringement.

That being said, the facts in this case, unlike *Frena, Sega,* and *Netcom,* are sufficient to establish that Defendants themselves engaged in two of the activities reserved to copyright owners under 17 U.S.C. § 106. The court finds that Defendants *distributed* and *displayed* copies of PEI photographs in derogation of PEI's copyrights. This finding hinges on two crucial facts: (1) Defendants' policy of encouraging subscribers to upload files, including adult photographs, onto the system, and (2) Defendants' policy of using a screening procedure in which RNE employees *viewed* all files in the upload file and *moved them* into the generally available files for subscribers.

These two facts transform Defendants from passive providers of a space in which infringing activities happened to occur to active participants in the process of copyright infringement. Defendants admit that they were operating a service where the quantity of adult files available to customers increased the attractiveness of the service. Defendants actively encouraged their subscribers to upload such files. Defendants had control over which files were discarded and which files were moved into the general system. Defendants knew that there was a possibility that PEI photographs were being uploaded onto the system, but failed to adopt

[Page 20]

procedures which ensured that any and all PEI photographs would be discarded. It is inconsistent to argue that one may actively encourage and control the uploading and dissemination of adult files, but cannot held liable for copyright violations because it is too difficult to determine which files infringe upon someone else's copyrights.

Distributing unlawful copies of a copyrighted work violates the copyright owner's distribution right and, as a result, constitutes copyright infringement. *Hotaling v. Church of Jesus Christ of Latter Day Saints,* 118 F.3d 199, 203 (4th Cir.1997). In order to establish "distribution" of a copyrighted work, a party must show that an unlawful copy was disseminated "to the public." *National Car Rental v. Computer Associates,* 991 F.2d 426, 434 (8th Cir.1993). The phrase "to the public," in this sense, includes paying subscribers to an otherwise publicly available service. *See Thomas v. Pansy Ellen Products,* 672 F.Supp. 237, 240 (W.D.N.C.1987) (display at trade show was public even though limited to members); *Ackee Music, Inc. v. Williams,* 650 F.Supp. 653 (D.Kan.1986) (performance of copyrighted songs at defendant's private club constituted public display). Defendants disseminated unlawful copies of PEI photographs to the public by adopting a policy in which RNE employees moved those copies to the generally available files instead of discarding them.

Similarly, Defendants violated PEI's right of public display. The comment to 17 U.S.C. Section106 states that a display is public if "it takes place 'at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances are gathered.' " H.R.Rep. No. 1476, 94th Cong., 2d Sess. 64 (Sept. 3, 1976), reprinted in U.S.Code Cong. & Admin. News 1976 p. 5659, 5677. "The same principles apply whenever the potential recipients of the transmission represent a limited segment of the public, such as the

[Page 21]

occupants of hotel rooms or the subscribers of a cable television service." *Id.* Defendants displayed copies of PEI photographs to the public by adopting a policy which allowed their employees to place those photographs in files available to subscribers.

Defendant RNE, the corporate owner of "Rusty-N-Edie's BBS," is liable for direct copyright infringement based on its policies of active participation in the infringing activities. This summary judgment is also applicable to President Russ Hardenburgh. Mr. Hardenburgh may not use the corporate veil as a defense to this action.

In *Southern Bell Tel. & Tel. v. Associated Tel. Directory Publishers,* 756 F.2d 801 (11th Cir.1985), the 11th Circuit Court of Appeals stated that "an individual, including a corporate officer, who has the

ability to supervise infringing activity and has a financial interest in that activity, or who personally participates in that activity is personally liable for the infringement." *Id.* at 811; *Vitabiotics, Inc. v. Krupka,* 606 F.Supp. 779, 785 (E.D.N.Y.1984) (holding an individual defendant jointly liable with three corporations active in marketing infringing materials). PEI has shown that Mr. Hardenburgh is the president and sole shareholder of the defendant corporation. (Hardenburgh dep. pp. 20-21.) Mr. Hardenburgh is also a paid employee of the corporation. (*Id.* at 62.) He has the sole ability to hire and fire employees on behalf of the corporation, and receives royalties paid to him by the corporation. (*Id.* at 56, 64-69.) Mr. Hardenburgh has the authority, right and ability to control the content of the BBS and its operations. (*Id.* at 73-91.) The summary judgment of direct copyright infringement is equally applicable to the corporation RNE and its President, Mr. Hardenburgh..

II.

Contributory Copyright Infringement

[Page 22]

A party shall be liable for contributory copyright infringement where it, "with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another." *Gershwin Publishing Corp. v. Columbia Artists,* 443 F.2d 1159, 1162 (2d Cir.1971). In *Sony Corp. v. Universal City Studios, Inc.,* 464 U.S. 417, 104 S.Ct. 774, 78 L.Ed.2d 574 (1984), the Supreme Court stated that:

> [t]he absence of such express language in the copyright statute does not preclude the imposition of liability for copyright infringement on certain parties who have not themselves engaged in the infringing activity. For vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold an individual liable for the actions of another.

Id. at 435.

The recent 9th circuit case of *Fonovisa, Inc. v. Cherry Auction, Inc.,* 76 F.3d 259 (9th Cir.1996) is instructive. In *Fonovisa,* the District Court had granted summary judgment in favor of defendant, who operated a "swap meet" where consumers purchased merchandise from individual and independent vendors. Plaintiff sued defendant for providing the space in which its copyrighted material was illegally sold, but the District Court concluded that there was no liability for contributory infringement where defendant had neither supervised nor directly profited from the vendors' sales. *Id.* at 262. The 9th Circuit reversed the District Court's dismissal, holding that contributory liability could attach where "infringing performances enhance the attractiveness of the venue to potential customers" *Id.* at 263; *Columbia Pictures Industries Inc. v. Aveco Inc.,* 800 F.2d 59 (3rd Cir.1986) (providing the site and facilities for known infringing activity is sufficient to establish contributory liability.)

In the present case, Defendants clearly induced, caused, and materially contributed

[Page 23]

to any infringing activity which took place on their BBS. Defendants admit that they encouraged subscribers to upload information including adult files. Defendants admit that they benefitted from having more files available to their customers. Also, Defendants had at least constructive knowledge that infringing activity was likely to be occurring on their BBS. Defendants were aware that PEI was enforcing its copyrights against BBS owners. Moreover, Playboy Magazine is one of the most famous and widely distributed adult publications in the world. It seems disingenuous for Defendants to assert that they were unaware that copies of photographs from Playboy Magazine were likely to find their way onto the BBS. Defendants are liable for contributory copyright infringement.

III.

Unfair Competition

Section 43(a) of the Lanham Act, 15 U.S.C. Section 1125(a), provides:

> (a)(1) Any person who, or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact which--
>
> > (A) is likely to cause confusion or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services or commercial activities by another person, or (B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities,
>
> shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

15 U.S.C. § 1125(a). The Sixth Circuit has not addressed the elements necessary to prove a

[Page 24]

Lanham Act claim. Recent case law establishes that the following must be shown in order to prevail: (1) the advertisements at issue are false or misleading and the advertisements actually deceived or had the tendency to deceive a substantial segment of the audience, (2) the deceptive or misleading portions of the advertisement were material, in other words they were likely to influence the purchasing decision, (3) defendant caused the advertised goods to enter interstate commerce, and (4) plaintiff has been or is likely to be injured either by direct diversion of sales from itself to defendant or by lessening the goodwill or acceptability its products enjoy with the buying public. *Telxon Corp. v. Symbol Technologies, Inc.*, 961 F.Supp. 1113, 1122 (N.D.Ohio 1996); *Hobart Corp. v. Welbilt Corp.*, 1989 WL 449696 (Oct. 4, 1989 N.D.Ohio) (quoting *Alpo Petfoods, Inc. v. Ralston Purina Co.*, 720 F.Supp. 194, 213 (D.D.C.1989) (citing *Skil Corp. v. Rockwell Int'l Corp.*, 375 F.Supp. 777, 783 (N.D.Ill.1974)); *U-Haul Int'l, Inc. v. Jartran, Inc.*, 522 F.Supp. 1238, 1243 (D.Ariz.1981), *aff'd*, 681 F.2d 1159 (9th Cir.1982)).

Plaintiff has failed to satisfy at least one of these elements, that the deceptive or misleading portions of the copied photographs were material, that is, likely to influence the purchasing decision of BBS subscribers. Plaintiff has not shown that subscribers to "Rusty-N-Edie's BBS" were drawn to that system because they believed that the adult photographs contained therein were created by Defendants. Plaintiff has not shown that Defendants made any attempt, or had any incentive, to pass off PEI photographs as if they were created by "Rusty-N-Edie's," other than to avoid copyright liability. Plaintiff will need to produce further evidence at trial to prevail on its Lanham Act claim that Defendants misled consumers about the source of the images.

Conclusion

For the reasons set forth above, Plaintiff's motion for summary judgment is granted on its claims of direct and contributory copyright infringement against Defendants. Plaintiff's motion for summary judgment is denied on its claim of unfair competition under the Lanham Act. All remaining claims shall be set forth for trial. A final pre-trial conference will take place on Monday, January 26, 1998 at 1:30 p.m. Jury trial shall be scheduled to begin on February 3, 1998, with the parties on two-week standby.

IT IS SO ORDERED.

/s/Judge Sam H. Bell
United States District Judge

FOOTNOTES:

1. For background information in this area, the court consulted a number of articles on the subject of computer bulletin boards and copyright infringement. *See* Keith Stephens & John P. Summer, *Catch 22: Internet Service Providers' Liability for Copyright Infringement over the Internet,* 14 No. 5 Computer Law I (1997); John Gladstone Mills III, *Entertainment on the Internet: First Amendment and Copyright Issues,* 79 J. Pat. & Trademark Off. Soc'y 46 I (1997); Joseph V. Myers, Note, *Speaking Frankly About Copyright Infringement on Computer Bulletin Boards: Lessons to be Learned from Frank Music, Netcom, and the White Paper,* 49 Vand. L.Rev. 439 (1996); Scott K. Pomeroy, Comment, *Promoting the Progress of Science and the Useful Arts in the Digital Domain: Copyright, Computer Bulletin Boards, and Liability for Infringement by Others,* 45 Emory L.J. 1035 (1996).

2. Defendants have not gone so far as to say that a finding of copyright liability in this case would result in a deprivation of their rights under the First Amendment. Defendants have rather asked the court to weigh the interests protected by the First Amendment in determining the applicability of the copyright statute to the facts before it.

E-LAW Locator E-LAW Home

http://www.Loundy.com/CASES/Playboy_v_Hardenburgh.html

PUBLISHED

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

KENNETH M. ZERAN, Plaintiff-Appellant,

v.

AMERICA ONLINE, INCORPORATED, Defendant-Appellee.

No. 97-1523

Appeal from the United States District Court for the Eastern District of Virginia, at Alexandria.

T. S. Ellis, III, District Judge.

(CA-96-1564-A)

Argued: October 2, 1997

Decided: November 12, 1997

Before WILKINSON, Chief Judge, RUSSELL, Circuit Judge, and BOYLE, Chief United States District Judge for the Eastern District of North Carolina, sitting by designation.

Affirmed by published opinion. Chief Judge Wilkinson wrote the opinion, in which Judge Russell and Chief Judge Boyle joined.

COUNSEL

ARGUED: John Saul Edwards, LAW OFFICES OF JOHN S. EDWARDS, Roanoke, Virginia; Leo Kayser, III, KAYSER & REDFERN, New York, New York, for Appellant.

Patrick Joseph Carome, WILMER, CUTLER & PICKERING, Washington, D.C., for Appellee.

ON BRIEF: John Payton, Samir Jain, WILMER, CUTLER & PICKERING, Washington, D.C.; Randall J. Boe, AMERICA ONLINE, INC., Dulles, Virginia, for Appellee.

OPINION

WILKINSON, Chief Judge:

Kenneth Zeran brought this action against America Online, Inc. ("AOL"), arguing that AOL unreasonably delayed in removing defamatory messages posted by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar postings thereafter. The district court granted judgement for AOL on the grounds that the Communications Decency Act of 1996 ("CDA") -- 47 U.S.C. Section(s) 230 -- bars Zeran's claims. Zeran appeals, arguing that Section(s) 230 leaves intact liability for interactive computer service providers who possess notice of defamatory material posted through their services. He also contends that Section(s) 230 does not apply here because his claims arise from AOL's alleged negligence prior to the

because his claims arise from AOL's alleged negligence prior to the CDA's enactment. Section 230, however, plainly immunizes computer service providers like AOL from liability for information that originates with third parties. Furthermore, Congress clearly expressed its intent that Section(s) 230 apply to lawsuits, like Zeran's, instituted after the CDA's enactment. Accordingly, we affirm the judgement of the district court.

I.

"The Internet is an international network of interconnected computers," currently used by approximately 40 million people worldwide. Reno v. ACLU, 117 S. Ct. 2329, 2334 (1997). One of the many means by which individuals access the Internet is through an interactive computer service. These services offer not only a connection to the Internet as a whole, but also allow their subscribers to access information communicated and stored only on each computer service's individual proprietary network. Id. AOL is just such an interactive computer service. Much of the information transmitted over its network originates with the company's millions of subscribers. They may transmit information privately via electronic mail, or they may communicate publicly by posting messages on AOL bulletin boards, where the messages may be read by any AOL subscriber.

The instant case comes before us on a motion for judgement on the pleadings, see Fed. R. Civ. P. 12(c), so we accept the facts alleged in the complaint as true. Bruce v. Riddle, 631 F.2d 272, 273 (4th Cir. 1980). On April 25, 1995, an unidentified person posted a message on an AOL bulletin board advertising "Naughty Oklahoma T-Shirts." The posting described the sale of shirts featuring offensive and tasteless slogans related to the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Those interested in purchasing the shirts were instructed to call "Ken" at Zeran's home phone number in Seattle, Washington. As a result of this anonymously perpetrated prank, Zeran received a high volume of calls, comprised primarily of angry and derogatory messages, but also including death threats. Zeran could not change his phone number because he relied on its availability to the public in running his business out of his home. Later that day, Zeran called AOL and informed a company representative of his predicament. The employee assured Zeran that the posting would be removed from AOL's bulletin board but explained that as a matter of policy AOL would not post a retraction. The parties dispute the date that AOL removed this original posting from its bulletin board.

On April 26, the next day, an unknown person posted another message advertising additional shirts with new tasteless slogans related to the Oklahoma City bombing. Again, interested buyers were told to call Zeran's phone number, to ask for "Ken," and to "please call back if busy" due to high demand. The angry, threatening phone calls intensified. Over the next four days, an unidentified party continued to post messages on AOL's bulletin board, advertising additional items including bumper stickers and key chains with still more offensive slogans. During this time period, Zeran called AOL repeatedly and was told by company representatives that the individual account from which the messages were posted would soon be closed. Zeran also reported his case to Seattle FBI agents. By April 30, Zeran was receiving an abusive phone call approximately every two minutes.

Meanwhile, an announcer for Oklahoma City radio station KRXO received a copy of the first AOL posting. On May 1, the announcer related the message's contents on the air, attributed them to "Ken" at Zeran's phone number, and urged the listening audience to call the number. After this radio broadcast, Zeran was inundated with death threats and other violent calls from Oklahoma City residents. Over the next few days, Zeran talked to both KRXO and AOL representatives. He also spoke to his local police, who subsequently surveilled his home to protect his safety. By May 14, after an Oklahoma City newspaper published a story exposing the shirt advertisements as a hoax and after KRXO made an on-air apology, the number of calls to Zeran's residence

finally subsided to fifteen per day.

Zeran first filed suit on January 4, 1996, against radio station KRXO in the United States District Court for the Western District of Oklahoma. On April 23, 1996, he filed this separate suit against AOL in the same court. Zeran did not bring any action against the party who posted the offensive messages.1 After Zeran's suit against AOL was transferred to the Eastern District of Virginia pursuant to 28 U.S.C. Section(s) 1404(a), AOL answered Zeran's complaint and interposed 47 U.S.C. Section(s) 230 as an affirmative defense. AOL then moved for judgment on the pleadings pursuant to Fed. R. Civ. P. 12(c). The district court granted AOL's motion, and Zeran filed this appeal.

II.

A.

Because Section(s) 230 was successfully advanced by AOL in the district court as a defense to Zeran's claims, we shall briefly examine its operation here. Zeran seeks to hold AOL liable for defamatory speech initiated by a third party. He argued to the district court that once he notified AOL of the unidentified third party's hoax, AOL had a duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future defamatory material. Section 230 entered this litigation as an affirmative defense pled by AOL. The company claimed that Congress immunized interactive computer service providers from claims based on information posted by a third party.

The relevant portion of Section(s) 230 states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. Section(s) 230(c)(1).2 By its plain language, Section(s) 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, Section(s) 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions -- such as deciding whether to publish, withdraw, postpone or alter content -- are barred.

The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum. In specific statutory findings, Congress recognized the Internet and interactive computer services as offering "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." Id. Section(s) 230(a)(3). It also found that the Internet and interactive computer services "have flourished, to the benefit of all Americans, with a minimum of government regulation." Id.Section(s) 230(a)(4) (emphasis added). Congress further stated that it is "the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." Id. Section(s) 230(b)(2) (emphasis added).

None of this means, of course, that the original culpable party who posts defamatory messages would escape accountability. While Congress acted to keep government regulation of the Internet to a minimum, it also found it to be the policy of the United States "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of

computer." Id. Section(s) 230(b)(5). Congress made a policy choice, however, not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages.

Congress' purpose in providing the Section(s) 230 immunity was thus evident. Interactive computer services have millions of users. See Reno v. ACLU, 117 S. Ct. at 2334 (noting that at time of district court trial, "commercial online services had almost 12 million individual subscribers"). The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.

Another important purpose of Section(s) 230 was to encourage service providers to self-regulate the dissemination of offensive material over their services. In this respect, Section(s) 230 responded to a New York state court decision, Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). There, the plaintiffs sued Prodigy -- an interactive computer service like AOL -- for defamatory comments made by an unidentified party on one of Prodigy's bulletin boards. The court held Prodigy to the strict liability standard normally applied to original publishers of defamatory statements, rejecting Prodigy's claims that it should be held only to the lower "knowledge" standard usually reserved for distributors. The court reasoned that Prodigy acted more like an original publisher than a distributor both because it advertised its practice of controlling content on its service and because it actively screened and edited messages posted on its bulletin boards.

Congress enacted Section(s) 230 to remove the disincentives to selfregulation created by the Stratton Oakmont decision. Under that court's holding, computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher. Fearing that the specter of liability would therefore deter service providers from blocking and screening offensive material, Congress enacted Section(s) 230's broad immunity "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." 47 U.S.C. Section(s) 230(b)(4). In line with this purpose, Section(s) 230 forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions.

B.

Zeran argues, however, that the Section(s) 230 immunity eliminates only publisher liability, leaving distributor liability intact. Publishers can be held liable for defamatory statements contained in their works even absent proof that they had specific knowledge of the statement's inclusion. W. Page Keeton et al., Prosser and Keeton on the Law of Torts Section(s) 113, at 810 (5th ed. 1984). According to Zeran, interactive computer service providers like AOL are normally considered instead to be distributors, like traditional news vendors or book sellers. Distributors cannot be held liable for defamatory statements contained in the materials they distribute unless it is proven at a minimum that they have actual knowledge of the defamatory statements upon which liability is predicated. Id. at 811 (explaining that distributors are not liable "in the absence of proof that they knew or had reason to know of the existence of defamatory matter contained in matter published").

Zeran contends that he provided AOL with sufficient notice of the defamatory statements appearing on the company's bulletin board. This notice is significant, says Zeran, because AOL could be held liable as a distributor only if it acquired knowledge of the defamatory statements' existence.

Because of the difference between these two forms of liability, Zeran contends that the term "distributor" carries a legally distinct meaning from the term "publisher." Accordingly, he asserts that Congress' use of only the term "publisher" inSection(s) 230 indicates a purpose to immunize service providers only from publisher liability. He argues that distributors are left unprotected bySection(s) 230 and, therefore, his suit should be permitted to proceed against AOL. We disagree. Assuming arguendo that Zeran has satisfied the requirements for imposition of distributor liability, this theory of liability is merely a subset, or a species, of publisher liability, and is therefore also foreclosed by Section(s) 230.

The terms "publisher" and "distributor" derive their legal significance from the context of defamation law. Although Zeran attempts to artfully plead his claims as ones of negligence, they are indistinguishable from a garden variety defamation action. Because the publication of a statement is a necessary element in a defamation action, only one who publishes can be subject to this form of tort liability. Restatement (Second) of Torts Section(s) 558(b) (1977); Keeton et al., supra, Section(s) 113, at 802. Publication does not only describe the choice by an author to include certain information. In addition, both the negligent communication of a defamatory statement and the failure to remove such a statement when first communicated by another party -- each alleged by Zeran here under a negligence label -- constitute publication. Restatement (Second) of Torts Section(s) 577; see also Tacket v. General Motors Corp., 836 F.2d 1042, 1046-47 (7th Cir. 1987). In fact, every repetition of a defamatory statement is considered a publication. Keeton et al., supra, Section(s) 113, at 799.

In this case, AOL is legally considered to be a publisher. "[E]very one who takes part in the publication . . . is charged with publication." Id. Even distributors are considered to be publishers for purposes of defamation law:

> Those who are in the business of making their facilities available to disseminate the writings composed, the speeches made, and the information gathered by others may also be regarded as participating to such an extent in making the books, newspapers, magazines, and information available to others as to be regarded as publishers. They are intentionally making the contents available to others, sometimes without knowing all of the contents -- including the defamatory content -- and sometimes without any opportunity to ascertain, in advance, that any defamatory matter was to be included in the matter published.

Id. at 803. AOL falls squarely within this traditional definition of a publisher and, therefore, is clearly protected bySection(s) 230's immunity.

Zeran contends that decisions like Stratton Oakmont and Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991), recognize a legal distinction between publishers and distributors. He misapprehends, however, the significance of that distinction for the legal issue we consider here. It is undoubtedly true that mere conduits, or distributors, are subject to a different standard of liability. As explained above, distributors must at a minimum have knowledge of the existence of a defamatory statement as a prerequisite to liability. But this distinction signifies only that different standards of liability may be applied within the larger publisher category, depending on the specific type of publisher concerned. See Keeton et al., supra, Section(s) 113, at 799-800 (explaining that every party involved is charged with publication, although degrees of legal responsibility

differ). To the extent that decisions like Stratton and Cubby utilize the terms "publisher" and "distributor" separately, the decisions correctly describe two different standards of liability. Stratton and Cubby do not, however, suggest that distributors are not also a type of publisher for purposes of defamation law.

Zeran simply attaches too much importance to the presence of the distinct notice element in distributor liability. The simple fact of notice surely cannot transform one from an original publisher to a distributor in the eyes of the law. To the contrary, once a computer service provider receives notice of a potentially defamatory posting, it is thrust into the role of a traditional publisher. The computer service provider must decide whether to publish, edit, or withdraw the posting. In this respect, Zeran seeks to impose liability on AOL for assuming the role for which Section(s) 230 specifically proscribes liability -- the publisher role.

Our view that Zeran's complaint treats AOL as a publisher is reinforced because AOL is cast in the same position as the party who originally posted the offensive messages. According to Zeran's logic, AOL is legally at fault because it communicated to third parties an allegedly defamatory statement. This is precisely the theory under which the original poster of the offensive messages would be found liable. If the original party is considered a publisher of the offensive messages, Zeran certainly cannot attach liability to AOL under the same theory without conceding that AOL too must be treated as a publisher of the statements.

Zeran next contends that interpreting Section(s) 230 to impose liability on service providers with knowledge of defamatory content on their services is consistent with the statutory purposes outlined in Part IIA. Zeran fails, however, to understand the practical implications of notice liability in the interactive computer service context. Liability upon notice would defeat the dual purposes advanced by Section(s) 230 of the CDA. Like the strict liability imposed by the Stratton Oakmont court, liability upon notice reinforces service providers' incentives to restrict speech and abstain from self-regulation.

If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement -- from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgement concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context. Cf. Auvil v. CBS 60 Minutes, 800 F. Supp. 928, 931 (E.D. Wash. 1992) (recognizing that it is unrealistic for network affiliates to "monitor incoming transmissions and exercise on-the-spot discretionary calls"). Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not. See Philadelphia Newspapers, Inc. v. Hepps, 475 U.S. 767, 777 (1986) (recognizing that fears of unjustified liability produce a chilling effect antithetical to First Amendment's protection of speech). Thus, like strict liability, liability upon notice has a chilling effect on the freedom of Internet speech.

Similarly, notice-based liability would deter service providers from regulating the dissemination of offensive material over their own services. Any efforts by a service provider to investigate and screen material posted on its service would only lead to notice of potentially defamatory material more frequently and thereby create a stronger basis for liability. Instead of subjecting themselves to further possible

lawsuits, service providers would likely eschew any attempts at selfregulation.

More generally, notice-based liability for interactive computer service providers would provide third parties with a no-cost means to create the basis for future lawsuits. Whenever one was displeased with the speech of another party conducted over an interactive computer service, the offended party could simply "notify" the relevant service provider, claiming the information to be legally defamatory. In light of the vast amount of speech communicated through interactive computer services, these notices could produce an impossible burden for service providers, who would be faced with ceaseless choices of suppressing controversial speech or sustaining prohibitive liability. Because the probable effects of distributor liability on the vigor of Internet speech and on service provider self-regulation are directly contrary to Section(s) 230's statutory purposes, we will not assume that Congress intended to leave liability upon notice intact.

Zeran finally contends that the interpretive canon favoring retention of common law principles unless Congress speaks directly to the issue counsels a restrictive reading of the Section(s) 230 immunity here. See United States v. Texas, 507 U.S. 529, 534 (1993). This interpretive canon does not persuade us to reach a different result. Here, Congress has indeed spoken directly to the issue by employing the legally significant term "publisher," which has traditionally encompassed distributors and original publishers alike.

The decision cited by Zeran, United States v. Texas, also recognized that abrogation of common law principles is appropriate when a contrary statutory purpose is evident. Id. This is consistent with the Court's earlier cautions against courts' application of the canon with excessive zeal: "`The rule that statutes in derogation of the common law are to be strictly construed does not require such an adherence to the letter as would defeat an obvious legislative purpose or lessen the scope plainly intended to be given to the measure.'" Isbrandtsen Co. v. Johnson, 343 U.S. 779, 783 (1952) (quoting Jamison v. Encarnacion, 281 U.S. 635, 640 (1930)); cf. Astoria Fed. Sav. & Loan Ass'n v. Solimino, 501 U.S. 104, 110-11 (1991) (statute need not expressly delimit manner in which common law principle is abrogated). Zeran's argument flies in the face of this warning. As explained above, interpreting Section(s) 230 to leave distributor liability in effect would defeat the two primary purposes of the statute and would certainly "lessen the scope plainly intended" by Congress' use of the term "publisher."

Section 230 represents the approach of Congress to a problem of national and international dimension. The Supreme Court underscored this point in ACLU v. Reno, finding that the Internet allows "tens of millions of people to communicate with one another and to access vast amounts of information from around the world. [It] is `a unique and wholly new medium of worldwide human communication.'" 117 S. Ct. at 2334 (citation omitted). Application of the canon invoked by Zeran here would significantly lessen Congress' power, derived from the Commerce Clause, to act in a field whose international character is apparent. While Congress allowed for the enforcement of "any State law that is consistent with [Section(s) 230]," 47 U.S.C. Section(s) 230(d)(3), it is equally plain that Congress' desire to promote unfettered speech on the Internet must supersede conflicting common law causes of action. Section 230(d)(3) continues: "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." With respect to federal-state preemption, the Court has advised: "[W]hen Congress has `unmistakably . . . ordained,' that its enactments alone are to regulate a part of commerce, state laws regulating that aspect of commerce must fall. The result is compelled whether Congress' command is explicitly stated in the statute's language or implicitly contained in its structure and purpose." Jones v. Rath Packing Co., 430 U.S. 519, 525 (1977) (citations omitted). Here, Congress' command is explicitly stated. Its exercise of its commerce power is clear and counteracts the caution counseled by the interpretive canon favoring retention of common law principles.

vested right in a non-final tort judgment, much less an unfiled tort claim. Hammond v. United States, 786 F.2d 8, 12 (1st Cir. 1986). Furthermore, Zeran cannot point to any action he took in reliance on the law prior to Section(s) 230's enactment. Because Section(s) 230 has no untoward retroactive effect, even the presumption against statutory retroactivity absent an express directive from Congress is of no help to Zeran here.

IV.

For the foregoing reasons, we affirm the judgement of the district court.

AFFIRMED

***** BEGIN FOOTNOTE(S) HERE *****

*fn1 Zeran maintains that AOL made it impossible to identify the original party by failing to maintain adequate records of its users. The issue of AOL's record keeping practices, however, is not presented by this appeal.

*fn2 Section 230 defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. Section(s) 230(e)(2). The term"information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." Id. Section(s) 230(e)(3). The parties do not dispute that AOL falls within the CDA's "interactive computer service" definition and that the unidentified third party who posted the offensive messages here fits the definition of an "information content provider."

***** END FOOTNOTE(S) HERE *****

available in the print version]

Copyright 1997 VersusLaw, Inc., (425) 250-0142

Home | Contents | Marketplace | News | Employment | Practice Areas | Resources | Law Tech. | Law Firms

Copyright © 1998, The New York Law Publishing Company. All Rights Reserved.
Access to Law Journal EXTRA! is governed by its Rules of Use. Send comments to feedback@ljextra.com